Allied Telesyn

Simply Connecting the World

AT-VP504E FXS (SIP/MGCP) VoIPTalk

Administration Manual

PN 990-11591-10 Rev C

Copyright © 2001 Allied Telesyn International, Corp.
960 Stewart Drive Suite B, Sunnyvale CA USA 94085

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn International, Corp.

Ethernet is a registered trademark of Xerox Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn International, Corp. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn International, Corp. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost of profit, arising out of or related to this manual or the information contained herein, even if Allied Telesyn International, Corp. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface

Introduction ix

Before you Begin ix
Acronyms ix
Related Documentation x
Manual Conventions xi

Part 1: Common Settings

Chapter 1

Getting Started 1

Overview 1
Why use the AT-VP504E FXS? 1
Implementing the AT-VP504E FXS Solution 2
Features 2
Panels 4
Front Indicators 4
Rear Connectors 5
What is SNMP? 6
SNMP Messages 7
What is a MIB? 7
MIB Structure 8
Changing a Parameter Value 8
Switching Protocols 9

Chapter 2

Installation 11

Hardware and Software Requirements 11
Package Contents 12
Choosing a Suitable Installation Site 12
Mounting the AT-VP504E FXS 13
Connecting the AT-VP504E FXS 17

Interpreting the AT-VP504E FXS LEDs 19
Test LED 19
LAN LED 19
Power LED 19
LED Behavior in Download Mode 20
Interpreting the LEDs in Reset Mode 20
Initial Provisioning Sequence 21
Troubleshooting During Provisioning 22
Using the Dual-Mode Default Settings Switch 22
Recovery Mode 22
Factory Settings Mode 24
Verifying the Installation 25

Chapter 3

Basic Configuration 27

Configuring the Software 27
Sending Configuration Data to the AT-VP504E FXS 28
Provisioning Sequence 29
Changing Software Variables 30
Setting the Location (Country) 30
Overriding the Country-Specific Settings 32
Placing a Call 33

Chapter 4

Network Configuration 35

Setting the Speed of the Ethernet Connection 35
Using DHCP (Dynamic) or Static Configuration 35
Using DHCP (Dynamic) Configuration 35
Using Static Configuration 37
Configuring the DHCP Server 38
Connection to the DHCP Behavior 38
Network Configuration 39
Creating Vendor Specific Information 39

Chapter 5

Software Download 43

Before Downloading 43
Configuring the TFTP Server 43
DHCP vs. Static Configuration 45
Download Procedure 46

LED States 48
Emergency Software Procedure 49
Downloading the Emergency Software 49
Using the Emergency Software 51

Chapter 6

System Failure Bypass Connector Configuration 53

System Failure Bypass Connector Settings 53
Setting the Bypass Service 53

Chapter 7

Port Configuration 55

Enabling Ports 55
Setting Basic DSP Variables 55
Setting User Gain Variables 57
Setting Country-Specific Variables 58
Selecting the Preferred Codec 59
Enabling Individual Codecs 59

Chapter 8

Unit Manager Configuration 61

Using the Unit Manager 61
DHCP vs. Static Configuration 62

Chapter 9

Miscellaneous Configuration 63

Using QoS 63
Differentiated Services (DS) Field 63
IEEE 802.1q 65
VLAN 66
Syslog Daemon Configuration 67
Why a Syslog Daemon? 67
DHCP vs. Static Configuration 68
Configuring the Syslog Daemon 69
SNMP Configuration 69
SNTP Settings 72
DHCP vs. Static Configuration 73

Selecting a Time Zone 74
Defining a Custom Time Zone 76

Chapter 10

Maintenance 79

Warning 79
Caution Regarding Handling 79
Location 79
Condensation 79
Cleaning 79
Troubleshooting 79
Solving General Operation Problems 80
Solving Software Upgrade Problems 81
Solving SNMP Management Software Problems 81

Part 2: SIP-Specific Settings

Chapter 11

Signalling Protocol Configuration – SIP 85

Setting up the SIP Logging Client 85
DHCP vs. Static Configuration 85
Setting up SIP User Agents Servers 86
DHCP vs. Static Configuration 86
Defining SIP User Agents 88
Authentication Information 89

Chapter 12

Telephony Configuration 91

Using Dial Maps 91
Using the Dial Map Special Characters 92
How to Use a Dial Map 92
Validating a Dial Map 94
Setting up Dial Maps 94
Dial Map Examples 96
Example 1 – Standard Calls 96
Example 2 – PBX Emulation 99

Supplementary Telephony Services 103
Call Forward 103
Call Waiting 106
Call Transfer – Supervised 106
Call Transfer – Unsupervised 106
Caller ID on Call Waiting 106
Three-Way Conference Call 106

Part 3: MGCP-Specific Settings

Chapter 13

Signalling Protocol Configuration – MGCP 109

Introduction 109
MGCP Information 109
Services Provided 110
Setting up Call Agents Information 110
DHCP vs. Static Configuration 110
Configuring Endpoints 112
Setting up Retransmission Parameters 112
Configuring Packages 114
Generic Media Package 114
DTMF Package 115
Line Package 115
Viewing Status Parameters 116
Viewing MGCP Statistics 117

Appendix A

Country Specific Parameters 119

Australia 119
Austria 119
France 120
Germany 120
Great Britain 121
Italy 122
Japan 122
North America 123
Spain 124
Switzerland 124

Appendix B

Safety & EMI Certifications 125

Safety & EMI Certifications Supported 125
Disclaimers 125
Federal Communications Commission (FCC) Part 15 125
Federal Communications Commission (FCC) Part 68 125
Industry Canada 126

Appendix C

Glossary 129

Introduction

The AT-VP504E FXS is a telephony adaptor that connects analog telephones or fax machines to a Local Area Network with access to an IP Network to permit high-quality, full duplex, audio/fax communications over IP Packet Networks.

Before you Begin

This manual provides all the information needed to install and manage the AT-VP504E FXS. It is intended for network administrators who install and set up network equipment; consequently, it assumes a basic working knowledge of LANs.

From the perspective of the LAN administrator, an AT-VP504E FXS presents itself just like another PC that is to be added to the LAN. It will require the same kind of TCP/IP addressing that is required by a PC. The AT-VP504E FXS can also use a DHCP server on the LAN to receive its IP configuration assignment automatically.

Acronyms

BORSCHT	Battery feed, Over-voltage protection, Ringing, Signalling, Coding, Hybrid, and Testing
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSP	Digital Signal Processor
FXS	Foreign Exchange Service
IP	Internet Protocol
ISDN	Integrated Services Digital Network

What's New in this Version

- 802.1q QoS priority tagging. See "IEEE 802.1q" on page 65 for more details.
- VLAN QoS priority tagging. See "VLAN" on page 66 for more details.
- Simple Network Time Protocol (SNTP). See "SNTP Settings" on page 72 for more details.
- Call transfer – Unsupervised. See "Call Transfer – Unsupervised" on page 106 for more details.

LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
PBX	Private Branch Exchange
PROM	Programmable Read-Only Memory
PSTN	Public-Switched Telephone Network
SCN	Switched Circuit Network
SIP	Session Initiation Protocol
SLIC	Subscriber's Line Interface Circuit
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network

Related Documentation

In addition to this manual, each document set of the AT-VP504E FXS includes the following:

- IP Communication Server Manual[1]

  This manual explains how to install and configure the IP Communication Server, which is a set of software tools that helps manage a network of VP500 communication units and other SIP devices. It also explains how to use the Unit Manager to remotely configure AT-VP504E FXS communication units.

  The manual is not printed – it is located on the documentation CD provided with the AT-VP504E FXS.

- AT-VP504E FXS User's Manual

  This manual provides information on how to use the AT-VP504E FXS. The manual is not printed – it is located on the documentation CD provided with the AT-VP504E FXS.

1. This is useful only if you have purchased the IP Communication Server.

- MIB Reference Manual

  Lists and explains all parameters in the MIB structure.

- AT-VP504E FXS Quick Start booklet

  This printed booklet allows you to quickly setup and work with the AT-VP504E FXS.

- IP Communication Server Quick Start booklet[1]

  This printed booklet allows you to quickly setup and work with the IP Communication Server.

Manual Conventions

This version of the AT-VP504E FXS can use either one of the following signalling protocols:

- the Session Initiation Protocol (SIP)
- the Media Gateway Control Protocol (MGCP)
- the Network-based Call Signaling (NCS)

To accommodate different settings in these signalling protocols, this manual is separated in three parts:

Table 1: Manual Parts

Part	Description
Part 1: Common Settings	Describes the settings that are valid on units running either the SIP or MGCP signalling protocol.
Part 2: SIP-Specific Settings	Describes settings exclusive to units running the SIP signalling protocol.
Part 3: MGCP-Specific Settings	Describes settings exclusive to units running the MGCP signalling protocol.

Part 1:
Common Settings

1 Getting Started

This chapter presents the AT-VP504E FXS. It describes the physical device and introduces the Simple Network Management Protocol (SNMP) as remote management tool.

Overview

The AT-VP504E FXS is a standalone Internet telephony terminal that connects to virtually any business telephone system supporting standard analog lines. It uses industry standard components and is designed for maximum system integration and scalability.

This version of the AT-VP504E FXS can use either one of the following signalling protocols:

- the Session Initiation Protocol (SIP), which is a simple signalling protocol for Internet conferencing and telephony.
- the Media Gateway Control Protocol (MGCP), which is a protocol for controlling Voice over IP (VoIP) Gateways from intelligent external call control elements.

  MGCP uses the Master/Slave concept, where external call control elements are the Masters, while the devices connected to them (such as the AT-VP504E FXS), are the Slaves and only obey orders given by the Master.

  The AT-VP504E FXS is used with any MGCP Call Agent (also known as Connection Manager), which manages calls from and to the AT-VP504E FXS.

You can switch from one signalling protocol to the other. See "MIB Structure" on page 8 for more information.

Why use the AT-VP504E FXS?

There are many reasons to use the AT-VP504E FXS:

- Merges voice and data traffic onto a single unified network.

  Carrying telephone traffic over data networks uses less bandwidth (as compared to telephone trunks), resulting in a more cost-effective network solution.
- Easily integrates with existing telephone equipment.
- Bypasses long-distance toll charges for realized savings.
- Supports 10 Mb/s and 100 Mb/s Ethernet networks.
- Upgrades software easily for future enhancements.
- Uses the latest standards in Internet Telephony.

- SIP or MGCP protocol for call management
- T.38 for fax relay

- Supports the following Codecs:
  - G.711 (µ-law, A-law)
  - G.723.1A
  - G.729 A rev. B
  - T.38 (fax) over UDP only
- Supports Quality of Service technologies.
  - Differentiated Services Field (DSCP)
  - IEEE 802.1q user priority tagging

Implementing the AT-VP504E FXS Solution

When an Internet telephony call is placed from one location to another, the voice signals pass through the AT-VP504E FXS. The voice signals are compressed into data packets, which are then diverted by the unit onto an IP/data network such as the Internet, or another type of data network. Upon reaching its destination, the data is converted back into voice signals, then fed into the corresponding endpoint.

The AT-VP504E FXS system utilizes technology that optimizes available bandwidth, so users do not hear echoes, stops and starts, or annoying clicks and pops. When traffic congestion is properly managed, AT-VP504E FXS customers cannot tell that their conversation is being carried over a packet network rather than the traditional Switched Circuit Network (SCN).

See the *AT-VP504E FXS User's Manuals* for call processes examples.

Features

The following table lists some of the features the AT-VP504E FXS offers.

Table 1: AT-VP504E FXS Features

Feature	Description
4 FXS Ports	Central Office quality SLICs supporting all the BORSCHT functions and thus meet most world wide telephony standards.

Table 1: AT-VP504E FXS Features (Continued)

Feature	Description
Fax Interface	Handles G3 and Super G3 fax transmissions at speeds up to 33.6 kbps. Automatic fax mode detection is standard on all ports. Real-Time Fax Over UDP with the T.38 protocol stack is also available.
Analog Modem	Supports 9.6 kbps to 33.6 kbps analog modems (V.34 support over clear channel).
System Failure Bypass	In the event of a commercial power failure or network failure, the system failure bypass feature permits users to make and receive calls even when the AT-VP504E FXS is not operating.
Full integration with the IP Communication Server[a]	After dialing a number, the AT-VP504E FXS contacts the IP Communication Server and the server looks through its internal database to translate the dialed number to a corresponding IP address. If there is no matching IP address associated to the dialed number, the IP Communication Server will look for a gateway willing to place a call to the dialed number on the SCN.
Fully Configurable “SCN-Like” Experience	The AT-VP504E FXS provides the tones heard on the standard telephone network. For example, a dial tone will be heard as soon as the handset is lifted. Call progress tones such as ringback and busy are also provided. The AT-VP504E FXS can be configured to take almost any kind of telephone number.
Remote Site Configuration/ Management	Integrates seamlessly into your existing administration environment. Implementation of a SNMP agent allows device-related adjustment parameters to be modified and polled remotely. The software upgrade (CPU and DSP code) is downloaded via a TFTP server.

a. Only valid for units that run the SIP signalling protocol.

Panels

This section provides an overview of the front and rear panels of the AT-VP504E FXS.

Front Indicators

Figure 1 shows the three (3) visual indicators located on the front of the AT-VP504E FXS.

Figure 1: Front Panel Indicators

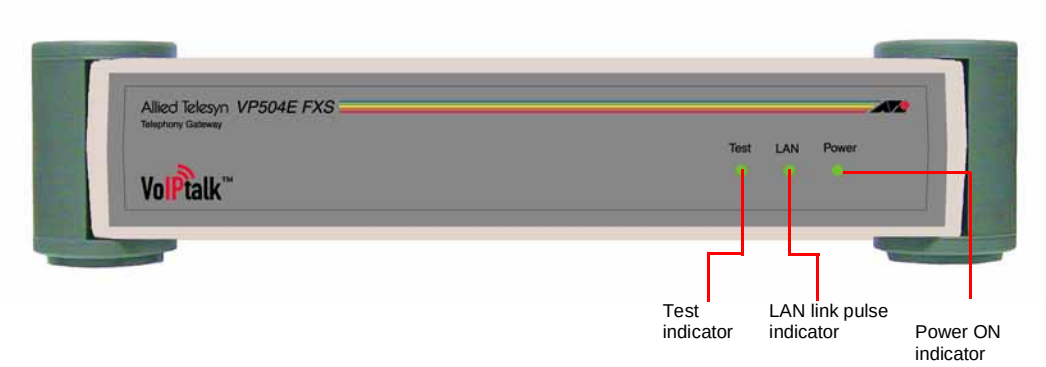


Table 2 describes the LEDs on the front panel of the AT-VP504E FXS.

Table 2: Front Panel Indicators

Indicator	Description
– **Test** – Test indicator	On when the AT-VP504E FXS is either running power up diagnostics or that it is in a maintenance state.
– **LAN** – LAN link pulse indicator	Provides the state of the network connected to the *Ethernet* port.
– **Power** – Power ON indicator	When lit, power is applied to the AT-VP504E FXS.

Rear Connectors

The AT-VP504E FXS has several connections that must be properly set. Figure 2 shows the back panel.

Figure 2: Back Panel Connectors

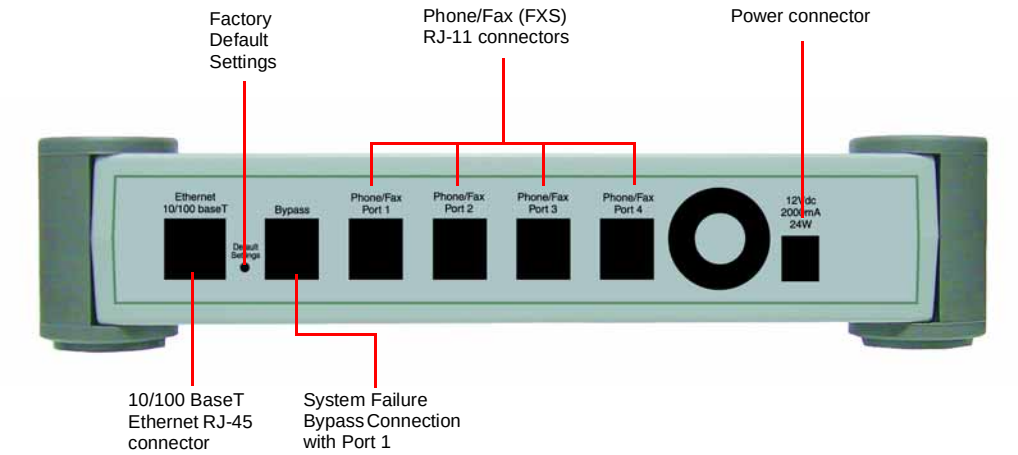


Table 3 describes the back panel connections.

Table 3: Connections of the AT-VP504E FXS

Connection	Description
Ethernet	A 10 BaseT Ethernet RJ-45 connector for access to a LAN.
System Failure Bypass	In the event of a commercial power failure or network failure, the system failure bypass feature permits users to make and receive calls even when the AT-VP504E FXS is not operating.
Phone/Fax Port 1 Phone/Fax Port 2 Phone/Fax Port 3 Phone/Fax Port 4	Four (4) RJ-11 connectors to attach a conventional telephone or G3/Super G3 fax machine.
Power connector	A power connector for the power supply of the AT-VP504E FXS.

Table 3: Connections of the AT-VP504E FXS (Continued)

Connection	Description
Default Settings switch	The *Default Settings* switch resets configuration parameters of the AT-VP504E FXS to default (known values). It can be used to reconfigure units. **Warning**: Read Section "Using the Dual-Mode Default Settings Switch" on page 22 before attempting to reset the unit.

What is SNMP?

The AT-VP504E FXS uses the Simple Network Management Protocol (SNMP) for initial software configuration provisioning and subsequent software configuration.

SNMP is a simple request-reply protocol for Internet network management services. It consists of *network management stations* (managers) communicating with *network elements*. The network elements can be anything that run the TCP/IP protocol suite: hosts, routers, X terminals (or in this case, an AT-VP504E FXS). The software in the network element that runs the management software is called the *agent*. Management stations are normally workstations that display relevant facts about the elements being monitored.

SNMP works over the IP (Internet Protocol) communication stack.

The communication can be two ways: the manager asking the agent for a specific value ("what is your designation?"), or the agent telling the manager that something important happened ("the AT-VP504E FXS has gone down"). Also, the manager can set variables in the agent in addition to reading variables from the agent.

TCP/IP network management consists of three pieces:

1. A *Management Information Base* (MIB) that specifies what variables the network elements maintain (the information that can be queried and set by the manager). See "What is a MIB?" on page 7 for more details.
2. A set of common structures and an identification scheme used to reference the variables in the MIB. This is called the *Structure of Management Information* (SMI).
3. The protocol between the manager and the element, called the *Simple Network Management Protocol* (SNMP). This details the format of the packets exchanged. Although a wide

variety of transport protocols could be used, UDP is normally used with SNMP.

SNMP Messages

SNMP defines only five types of messages that are exchanged between the manager and agent.

Table 4: SNMP Message Types

Operator	Description
get-request	Fetch the value of one or more variables.
get-next-request	Fetch the next variable after one or more specified variables.
set-request	Set the value of one or more variables.
get-response	Return the value of one or more variables. This is the message returned by the agent to the manager in response to the **get-request**, **get-next-request**, and **set-request** operators.
trap	Notify the manager when something happens on the agent.

The first three messages are sent from the manager to the agent, and the last two are from the agent to the manager.

What is a MIB?

A *Management Information Base* (MIB) specifies what variables the network elements maintain (the information that can be queried and set by the manager). All variables are identified by object identifiers, a hierarchical naming scheme consisting of long strings of numbers that are normally abbreviated into a simple name, for human readability.

A MIB is structured like a tree. At the top of the tree is the most general information available about a network. Each branch of the tree then gets more detailed into a specific network area, with the leaves of the tree as specific as the MIB can get.

MIB Structure

The current Allied Telesyn MIB structure has three individual MIB modules:

Table 5: Allied Telesyn MIB Structure

MIB	Description
Provisioning MIB	Allows you to set up all the parameters related to the AT-VP504E FXS communication unit. The Provisioning MIB contains all the functional parameters the unit uses to operate.
MGCP MIB	Used exclusively with AT-VP504E FXS communication units that run the Media Gateway Control Protocol (MGCP).
SIP MIB	Used exclusively with AT-VP504E FXS communication units that run the Session Initiation Protocol (SIP).

Figure 3: MIB Structure

All parameters in the MIBs have been configured by default upon start up. However, if you need to modify some of these parameters (for example, parameters related to the country in which you are), use a SNMP browser.

Changing a Parameter Value

Modifying a parameter involves contacting the AT-VP504E FXS communication unit with any SNMP MIB browser. Be sure to use the MIB modules that match the version of those located inside the current software build of the unit.

You can use the built-in SNMP editor of the Unit Manager. See the *IP Communication Server Administration Manual* for more details. You can also use the Unit Manager Express, a free MIB browser located on the documentation CD provided with your AT-VP504E FXS communication unit.

You must then locate the proper parameter to modify and change its value. Most of the parameters will require that you reboot the AT-VP504E FXS communication unit. A reboot may be software-initiated or manually initiated with the power connector. It will delete all statistics stored and will overwrite all volatile parameter values in the configuration file. A reboot will also reinitiate the entire unit's initial provisioning sequence.

Switching Protocols

The MIB structure contains three MIB modules, but only two are actually used at the same time:

- With the SIP signalling protocol: the AT-VP504E FXS uses the Provisioning MIB and SIP MIB.
- With the MGCP signalling protocol: the AT-VP504E FXS uses the Provisioning MIB and MGCP MIB.

You can switch between protocols and the proper MIB will be activated upon restart.

To switch MIB according to the protocol used:

1. In the general Provisioning MIB, locate the *signaling ProtocolsSwitch* variable under the *signaling ProtocolsGroup*.

   This variable allows you to switch from one protocol to another.

2. Set the *signalingProtocolsSwitch* variable to either **0=MGCP** or **1=SIP**

   The default value is **1=SIP**. The AT-VP504E FXS communication unit reboots automatically. After the unit restarts, it will use the selected MIB. See:

   - "Part 2: SIP-Specific Settings" on page 83
   - "Part 3: MGCP-Specific Settings" on page 107

2 Installation

This chapter explains the requirements for installing the AT-VP504E FXS and describes the installation and the initial provisioning of the AT-VP504E FXS.

Hardware and Software Requirements

The AT-VP504E FXS requires the following items:

Table 6: AT-VP504E FXS Required Items

Item	Description
Phone or Fax	A standard telephone or fax attached to an FXS port. You can attach up to four phones or faxes to the AT-VP504E FXS.
Remote Termination / Endpoints	Other endpoints on the IP network where the AT-VP504E FXS terminates a call. For example, it could be: • a standard telephone/fax attached to a terminal such as an AT-VP504E FXS • a Soft Phone • an IP phone directly connected to the IP network • etc.
DHCP Server	Supplies all network parameters to the AT-VP504E FXS such as the IP address and subnet mask. **Note**: The DHCP server is used only for automatic configuration.
Call Agent[a]	Manages the active calls of the AT-VP504E FXS.
TFTP Server	Necessary for software updates.
Syslog Daemon (optional)	Receives all status messages coming from the AT-VP504E FXS. It keeps the administrator informed of any warning or error messages sent by the AT-VP504E FXS. See “Syslog Daemon Configuration” on page 67 for more details.

a. Only valid for units that run the MGCP or NCS signalling protocol.

Package Contents

Your AT-VP504E FXS package contains the following items:

- the AT-VP504E FXS communication unit
- 4 rubber feet for the AT-VP504E FXS
- a power supply for the country in which you will be using the AT-VP504E FXS
- a CD that contains an Administration Manual, a MIB Reference Manual, a User's Manual and an IP Communication Server Manual
- a Quick Start booklet

Choosing a Suitable Installation Site

The AT-VP504E FXS is suited for use in an office environment where it can be wall-mounted, mounted on a standard 48.26 cm (19 in.) equipment rack, or free standing on its rubber feet. In addition, the AT-VP504E FXS can be rack-mounted in a wiring closet or equipment room.

Note: The wall-mounting or rack-mounting kit is not part of the standard AT-VP504E FXS package and must be ordered separately.

When deciding where to position the AT-VP504E FXS, ensure that:

- The AT-VP504E FXS is accessible and cables can be easily connected.
- The cabling is away from the following:
  - Sources of electrical noise such as radios, transmitters, and broadband amplifiers
  - Power lines and fluorescent lighting fixtures
  - Water or moisture that could enter the casing of the AT-VP504E FXS.
- The airflow is not restricted around the AT-VP504E FXS or through the vents in the side of the unit. It is necessary to have a minimum of 25 mm (1 in.) clearance.
- The fan on the AT-VP504E FXS is not blocked or that the back of the unit is not too close to the wall.
- No more than four (4) AT-VP504E FXS units are placed on top of one another, if the units are free standing.

Mounting the AT-VP504E FXS

Rack-Mounting the AT-VP504E FXS

The AT-VP504E FXS is 5.5 cm (2.2 in.) high and fits in most standard 48.26 cm (19 in.) racks. Allied Telesyn recommends that you use a rack compliant EIA-310-D.

▶ **To rack-mount the AT-VP504E FXS:**

1. Disconnect all of the cables from the AT-VP504E FXS.
2. Remove all of the rubber feet from the AT-VP504E FXS, if applicable.
3. Place the AT-VP504E FXS right side up on a hard flat surface, with the front facing toward you.
4. Place the left mounting bracket over the mounting holes on the left side of the AT-VP504E FXS. Figure 4 illustrates the rack-mounting pieces.

Figure 4: Rack mounting pieces

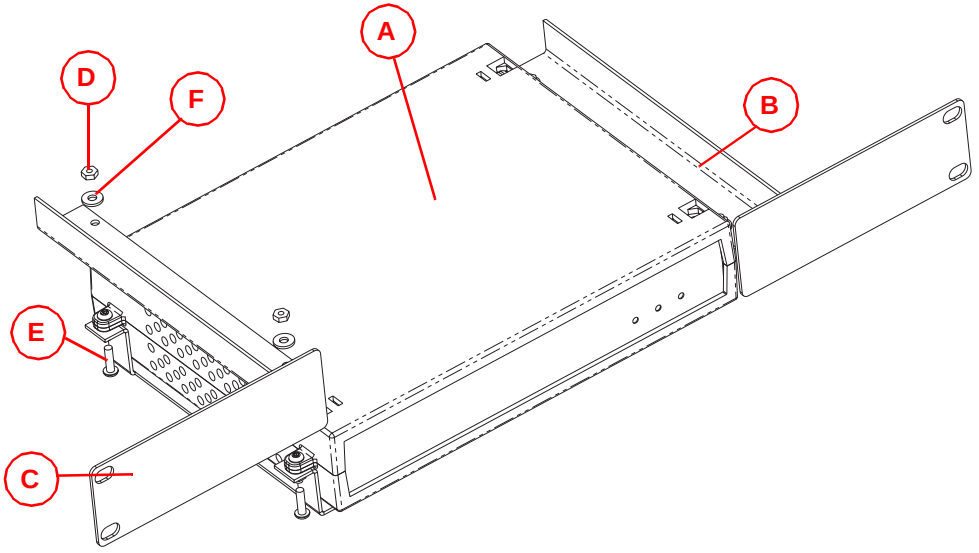


Table 7 describes the rack-mounting pieces illustrated in Figure 4.

Table 7: Rack-Mounting Pieces

Item No.	Qty.	Description
A	1	AT-VP504E FXS casing

Table 7: Rack-Mounting Pieces (Continued)

Item No.	Qty.	Description
B	1	Right rack-mount bracket (already installed in Figure 4)
C	1	Left rack-mount bracket
D	4	6 x 32 5/16 across 7/64 thick steel Hex machine screw nuts
E	4	6 x 32 UNC 1/2 steel philips binding head screws
F	4	6 bolt size split lock washers

The left and right mounting brackets are not identical. Therefore, make sure that you use the proper bracket.The bracket should be perfectly aligned with the side of the AT-VP504E FXS.

5. Insert the two screws in the left mounting bracket, and tighten.

Note: You must use the screws supplied with the mounting brackets. Damage caused to the unit by using incorrect screws invalidates your warranty.

6. Repeat steps 4 and 5 for the other side of the AT-VP504E FXS.
7. Insert the AT-VP504E FXS into the bracket and secure with suitable screws (not provided). Make sure that the ventilation holes are not obstructed.
8. Connect the cabling as per “Connecting the AT-VP504E FXS” on page 17.

Wall-Mounting the AT-VP504E FXS

A single AT-VP504E FXS can be wall-mounted.

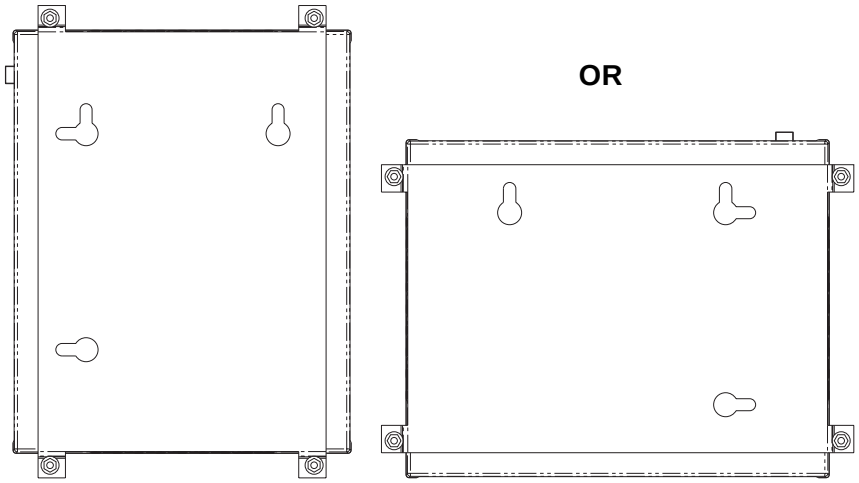
▶ **To wall-mount the AT-VP504E FXS:**

1. Disconnect all of the cables from the AT-VP504E FXS before mounting.
2. Ensure that the wall you are using is smooth, flat, dry and sturdy. Attach a piece of plywood, approximately 305 mm x

510 mm x 12 mm (12 inches x 20 inches x 0.5 inches) securely to the wall, if necessary.

3. Position the wall-mounting bracket against the wall (or plywood) and ensure that one of the sides with two screw holes faces the sides or the top (see Figure 5). **Do not position the side with two screw holes downward**. Mark the position of the screw holes on the wall. Drill the two holes.

Figure 5: Wall Mounting bracket



4. Insert suitable brackets and screws (not provided) to the wall or plywood. Attach the wall-mounting bracket to the screws to ensure that the bracket is secure.

5. Remove the wall-mounting bracket from the wall and place it right side up on a hard flat surface with the front (the side that has two screw holes) facing toward you.

6. Remove all of the rubber feet from the AT-VP504E FXS, if applicable.

7. Place the AT-VP504E FXS right side up on the wall-mounting bracket, with the front facing toward you.

8. Place the AT-VP504E FXS screw holes on the side over the mounting holes of the wall bracket. See Figure 6 for the location of the wall-mounting pieces.

Figure 6: Fitting the wall bracket for wall-mounting

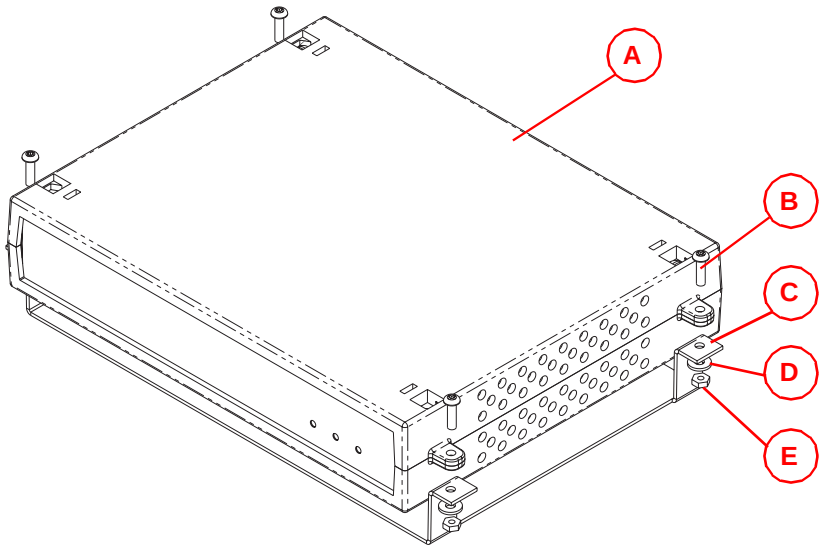


Table 8 describes the wall-mounting pieces illustrated in Figure 6.

Table 8: Wall-Mounting Pieces

Item	Qty.	Description
A	1	AT-VP504E FXS casing
B	4	6 x 32 UNC 1/2 steel philips binding head screws
C	1	Wall-mounting bracket
D	4	6 bolt size split lock washers
E	4	6 x 32 5/16 across 7/64 thick steel Hex machine screw nuts

9. Insert the four screws into the screw holes, and tighten.

10. Place the wall-mounting bracket on the wall and place the screw holes of the wall-mounting bracket over the screws installed in step 4.

Note: Ensure that the AT-VP504E FXS's front faces the sides or the top. **Do not position the front of the AT-VP504E FXS downward**. If the AT-VP504E FXS's front faces downwards, the wall-mounting bracket is not installed properly. See step 3.

11. Connect the network cabling as per "Connecting the AT-VP504E FXS" on page 17.

Stacking Units on Top of Each Other

For free-standing AT-VP504E FXS units, you can stack up to four units on top of each other. If you are mixing a variety of hub units, position the smaller units at the top.

If you are stacking AT-VP504E FXS units, you must use the supplied rubber feet. Insert the rubber feet into the tabs on either sides of the AT-VP504E FXS. Place the AT-VP504E FXS units on top of each other. Make sure that the feet of the upper unit line up with the recesses of the lower unit.

Warning: Stacking more than four (4) units on top of the other may overheat the AT-VP504E FXS.

Connecting the AT-VP504E FXS

This section describes how to set the connectors of the AT-VP504E FXS. Figure 7 on page 18 illustrates the connectors that correspond to the steps.

Warning: Do not connect the AT-VP504E FXS directly to Analog Telephone Systems.

▶ **To connect the AT-VP504E FXS hardware:**

1. analog telephones or fax machines into Ports 1, 2, 3, and 4.

Note: The AT-VP504E FXS telephone line interface has been designed to interface with a conventional telephone line. Connections to certain PBX / Key systems supply a higher line voltage that could damage the AT-VP504E FXS.

2. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *Ethernet* connector of the AT-VP504E FXS and connect the other end to a compatible Ethernet interface that supplies

TCP/IP network access (e.g. router, switch, hub or computer).

You must also install the IP Communication Server[1] on a machine accessible by the network in order to take full advantage of the AT-VP504E FXS. Please refer to the IP Communication Server Manual for more details on how to install and configure it.

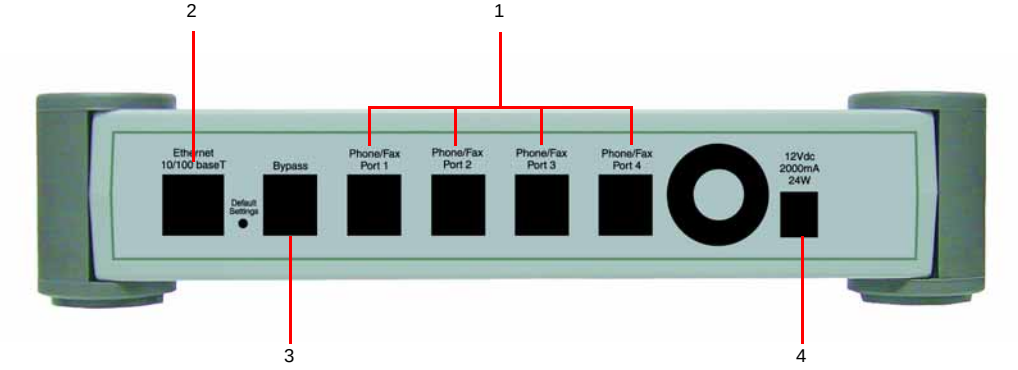
3. Connect a SCN line into the *Bypass* port of the AT-VP504E FXS (optional).

4. Connect the power supply to the AT-VP504E FXS and then connect the power cable to an electrical outlet.

Warning: The electrical outlet shall be installed near the AT-VP504E FXS so that it is easily accessible.

5. Turn the AT-VP504E FXS on.

Figure 7: Steps for Connecting the AT-VP504E FXS Hardware



1. Only valid for units that run the SIP signalling protocol.

Interpreting the AT-VP504E FXS LEDs

The AT-VP504E FXS has three (3) LED indicators located on the front panel, which are identified as *Test*, *LAN*, and *Power*. A LED has three states: On, Off and Blinking.

Test LED

The *Test* LED indicates if a phone/fax connected to one of the *Phone* ports is off hook or on hook.

LAN LED

The *LAN* LED provides the status of the network connected to the *Ethernet* port. Normal operation is variable On-Off blinking.

Table 9: LAN LED Status

Operation	LED Status	Description
link_down	Steady OFF	*Ethernet* port does not sense the carrier signal.
link_up	Steady ON	Only valid for the first 4 seconds after initial receipt of carrier signal.
link_active	Variable Blinking	It is on when data is transmitted or received on the *Ethernet* port. This implies that the LINK_UP is also true.

Power LED

The *Power* LED is used to indicate whether the AT-VP504E FXS is operational at its most basic level. It does not imply that the unit can be used, only that it is capable of being used. Normal operation is steady On.

Table 10: Power LED Status

Operation	LED Status	Description
normal	Steady ON	Power is on and the unit does not have any major failure.
failed	3 HZ Blinking at 50% ON duty cycle	Failure of power-up diagnostics such that the unit is unable to operate.
addr_fail	1 HZ Winking at 75% ON duty cycle	Failure of DHCP – no acceptable offer received from DHCP.
no_power	Steady OFF	The unit has no power supply input.

LED Behavior in Download Mode

When the AT-VP504E FXS initiates a software download, the three LEDs located on the front panel are used to report the status of the process:

Table 11: LED States in Software Download

Event	LED State
IMAGE_DOWNLOADING (download phase)	Each LED blinks alternately at 1 Hz with 1/3 ON duty cycle.
IMAGE_WRITING (writing to EEPROM phase)	*Test* LED ON, *LAN* LED ON, *Power* LED OFF. **Warning**: Do not turn the AT-VP504E FXS off while in this state.
IMAGE_UPDATE_FAIL	All LEDs blink at the same time at 2 Hz with 50% ON duty cycle for 5 seconds.
IMAGE_UPDATE_SUCCESS	All LEDs ON.

Interpreting the LEDs in Reset Mode

When resetting the AT-VP504E FXS at boot time, the three LEDs start blinking. If you hold the *Default Settings* switch less than 15 seconds, the IP address of the unit will default to the static value 192.168.0.1. If you want the unit to use a DHCP-provided address, you will then have to set the *interfaceUseDhcp* Provisioning MIB variable to **1** and reboot the unit.

If you hold the *Default Settings* switch at least 15 seconds, the three LEDs will stop blinking – remaining ON – indicating that the MIB database and the rescue application's file have been rebuilt and default values set. Upon releasing the *Default Settings* switch, the AT-VP504E FXS will reboot. See "Using the Dual-Mode Default Settings Switch" on page 22 for more information.

Initial Provisioning Sequence

When powering the AT-VP504E FXS for the first time, it needs to be configured before it can support calls. This process is known as *provisioning*. There are several components involved in provisioning.

This sequence assumes that you have installed the AT-VP504E FXS hardware and connected it to a compatible Ethernet interface that supplies TCP/IP network access (e.g. router, switch, hub or computer).

Note: The AT-VP504E FXS requests its configuration only on the first boot.

▶ **Initial provisioning sequence:**

1. When the AT-VP504E FXS boots, it broadcasts a message requesting DHCP services.
2. The DHCP server responds with a set of IP addresses and network parameters, one of which is the AT-VP504E FXS IP address.

   The following are some of the network parameters assigned via DHCP:

   - AT-VP504E FXS IP address
   - Subnet Mask
   - Default Router IP address
   - Primary DNS IP address
   - Secondary DNS IP address
   - Unit Manager IP address
   - Unit Manager IP port number
3. The AT-VP504E FXS uses the IP address of the Unit Manager to request its configuration.
4. The Unit Manager configures the AT-VP504E FXS.

Troubleshooting During Provisioning

If contact is not established properly with the various agents involved, see the following Table for possible problems and solutions:

Table 12: Troubleshooting During Provisioning

Problem	Solution
DHCP does not answer	If, after 5 requests in 20 seconds, the DHCP does not answer, the AT-VP504E FXS stops requesting DHCP offers. You must then set the IP addresses and network parameters through static values.
Unit Manager does not answer	If the Unit Manager does not answer before the retry count elapses, the AT-VP504E FXS stops the provisioning sequence. If the AT-VP504E FXS does not use any Unit Manager address, it stops the provisioning sequence.

Using the Dual-Mode Default Settings Switch

You can use the dual-mode *Default Settings* switch on the back of the AT-VP504E FXS in two different ways:

- Pressing the *Default Settings* switch for less than 15 seconds at startup will boot the AT-VP504E FXS in “Recovery Mode”.
- Pressing the *Default Settings* switch at startup for at least 15 seconds will apply the “Factory Settings” procedure. This feature will permit to revert back to the default factory settings of the AT-VP504E FXS.

You should use the dual-mode *Default Settings* switch only in case of emergencies, i.e. when the AT-VP504E FXS refuses to work properly for any reason or the connection to the network is lost.

Recovery Mode

Using the *Default Settings* switch in Recovery mode will assign a static default IP address.

▶ **To use the *Default Settings* switch in Recovery Mode:**

1. Power the AT-VP504E FXS off by unplugging the power connector.
2. With a 10/100 Hub and two (2) 10/100 BaseT Ethernet RJ-45 straight cables, connect both cables to the Hub; one of them

is connected into the *Ethernet* connector of the AT-VP504E FXS and the other one links the computer to the Hub.

Alternatively, you can connect a **10/100 BaseT Ethernet RJ-45 crossover cable** into the *Ethernet* connector of the AT-VP504E FXS and connect the other end to your computer.

You must perform the recovery mode in a closed network. You must also perform it on only one AT-VP504E FXS at a time, since the default IP address is the same on every unit.

3. If you are using Windows, access *Start/Settings/Control Panel/Network*. In the *Protocols* tab, highlight the TCP/IP protocol and click *Properties.*

4. Select the network adapter you are about to assign a static IP address to.

   In the *IP address* tab, choose *Specify an IP address*. Enter the IP Address of *192.168.0.10* and the Subnet Mask of *255.255.255.0*. Close all the windows and reboot your computer.

5. Insert a small paper clip into the *Default Settings* switch hole of the AT-VP504E FXS. While depressing the *Default Settings* switch, power the unit on.

   The electrical outlet shall be installed near the AT-VP504E FXS so that it is easily accessible. All three LEDs should stop blinking, staying ON to inform you that the recovery reset has been performed.

Note: Hold the *Default Settings* switch just a few seconds (less than 15 seconds).

In recovery mode, the following default parameters are statically assigned to the AT-VP504E FXS:

- **Default local IP address**: 192.168.0.1
- **Default subnet mask**: 255.255.255.0

All the MIB parameters except *interfaceUseDhcp* are kept.

In this mode, SIP/MGCP is deactivated. Only SNMP can be used to set any appropriate parameter value, especially the IP address.

6. When the AT-VP504E FXS has finished its provisioning sequence, set the *interfaceUseDhcp* variable to **1**, then turn it off, plug it on the network, and turn it on again.

Note: The recovery mode does not alter any persistent configuration data of the AT-VP504E FXS, except the *interfaceUseDhcp* variable.

Factory Settings Mode

This procedure allows to revert back to the default factory settings of the AT-VP504E FXS. It deletes the MIB database of the unit and creates a new configuration file with the default factory values. It should be performed with the AT-VP504E FXS connected to a network with access to a DHCP server. If the unit cannot find a DHCP server, it will use the static address 192.168.0.1. In this case, your PC must use the static IP address 192.168.0.10.

▶ **To use the *Default Settings* switch in Factory Settings mode:**

1. Power the AT-VP504E FXS off.
2. Insert a small paper clip into the *Default Settings* switch hole of the AT-VP504E FXS. While pressing the *Default Settings* switch, power the unit on.

   The electrical outlet shall be installed near the AT-VP504E FXS so that it is easily accessible. You must keep pressing the paper clip for at least 15 seconds. Do not depress before the three LEDs stop blinking and are steadily ON.
3. Release the paper clip.

   The AT-VP504E FXS restarts.

   This procedure resets all variables in the MIB modules to their default value; defaults include the *interfaceUseDhcp* variable set to **1**.

   When the AT-VP504E FXS has finished its provisioning sequence, it is ready to be used with a DHCP-provided IP address and MIB parameters.

Note: The factory default settings mode does alter any persistent configuration data of the AT-VP504E FXS. The MAC address is re-written with its own value.

Verifying the Installation

There are two ways to verify that the AT-VP504E FXS is properly connected to the IP network and is working:

- By contacting it with a SNMP Browser
- By pinging it

These two procedures assume that you know the IP address of the AT-VP504E FXS you want to verify. If the AT-VP504E FXS does not respond, do the following:

- Verify that the LAN cable is securely connected to the AT-VP504E FXS and to the network connector.
- Make sure that you did not connect a cross-over network cable.
- Verify the state of the IP network to ensure it is not down (the *LAN* LED should be ON or blinking).
- Verify that the registrar server redirect/proxy server are both operational[2].
- Verify that the primary and secondary call agents are both operational[3].

2. Only valid for units that run the SIP signalling protocol.
3. Only valid for units that run the MGCP signalling protocol.

3 Basic Configuration

This chapter describes how to configure the AT-VP504E FXS for basic operation.

Configuring the Software

The AT-VP504E FXS software parameters are fully programmable using the SNMP protocol. There are two ways to set up and configure a unit:

- By using a SNMP browser to contact the MIBs of the AT-VP504E FXS.

  This manual explains how to use any third-party SNMP browser to monitor and configure the AT-VP504E FXS, provided the correct MIB structure is installed on the management workstation. You can use any SNMP browser or network management application running the SNMP protocol. However, the information may not be presented in the same manner depending on the SNMP browser used.

Note: It is assumed that you have basic knowledge of TCP/IP network administration.

Network Management

When managing an AT-VP504E FXS over the network, the unit must be correctly configured with an IP address and a subnet mask.

IP Addresses

To operate correctly, each unit on a network must have a unique IP address. IP addresses have the format *n.n.n.n* where *n* is a decimal number between 0 and 255, for example, *192.168.0.1*. If your network has a connection to the external IP network, you need to apply for a registered IP address. This system ensures that each IP address is unique; if you do not have a registered IP address, you may be using an address identical to someone else's and your network may not operate correctly.

Subnets and Using a Subnet Mask

You can divide your IP network into sub-networks or subnets. Support for subnets is important because the number of bits assigned to the device part of an IP address limits the number of devices that may be addressed on any given network. For example, a Class C address is restricted to 254 devices.

Note: If you have a small network (less than 254 devices), you may decide not to have subnets.

If you are unsure about what mask to use, Allied Telesyn suggests that you use a general mask, *255.255.255.0*, which corresponds to the example address used in the previous sections.

- By using the user interface of the IP Communication Server.

  See the *IP Communication Server Administration Manual* for more details on how to use it to configure any AT-VP504E FXS communication unit on the network.

Please refer to the *MIB Reference* manual for a complete list of variables that can be set.

Sending Configuration Data to the AT-VP504E FXS

The configuration data that must be provisioned into the AT-VP504E FXS can be supplied in two ways:

- as a configuration file sent from the Unit Manager to the AT-VP504E FXS via TFTP
- as a MIB sent from the Unit Manager to the AT-VP504E FXS via SNMP

Configuration File

The configuration file has the advantage of being the fastest way to deliver the necessary information. This may be important in the situation where you must initialize a large number of units at the same time. However it has one serious disadvantage: the file must be sent all at the same time and individual variables cannot be changed without sending a whole new file. The configuration file is mostly used for the initial provisioning sequence (see “Initial Provisioning Sequence” on page 21 for more details).

It is also possible to request a configuration file by setting the following two Provisioning MIB variables:

- apaCmdRequestConfiguration = 1
- apaCmdConfigurationMode = -1

The Unit Manager, if properly set up, can send a new configuration file at any time you want. This could be used to update the MIB variables all at the same time. This requires to reboot the AT-VP504E FXS.

The configuration file format is like a Microsoft *.INI* file, except that the value is enclosed by two double quotes (even for numbers) and there is no section marker [section].

Normally, there is only one attribute assignment per line. A carriage return line feed character (CRLF) terminates each line. To put some comments, you can use the character # as the first character on the line. In this case, the entire line will be ignored.

On each line, you can assign a value to an attribute by using this syntax:

```
<mibAttributeName> = "<mibAttributeValue>"
```

Example of a Configuration File

```
interfaceUseDhcp="1"
interfaceStaticPrimDnsIp="192.168.0.10"
interfaceStaticSecDnsIp="192.168.0.10"
interfaceStaticDefaultRouterIp="192.168.0.10"
interfaceStaticSubnetMaskIp="255.255.255.0"
apaManagerEnable="1"
apaManagerUseDhcp="1"
apaManagerStaticPrimHost="192.168.0.10"
apaManagerStaticPrimTrapPort="162"
tftpFileName="vp500.bin"
tftpEmergencyFileName="vp500_emergency.bin"
tftpUseDhcp="1"
tftpServerStaticHost="192.168.0.10"
tftpServerStaticPort="69"
tftpServerStaticEmergencyHost="192.168.0.10"
tftpServerStaticEmergencyPort="69"
```

Management Information Base – MIB

Sending information as a MIB via SNMP means that individual variables could be changed without sending the whole MIB. You could use a dual system where a configuration file is sent for initial configuration and a MIB is used to implement minor changes.

The AT-VP504E FXS has three configurable MIBs: the Provisioning MIB, SIP MIB and MGCP MIB. All variables in these MIBs have been configured by default upon start up. However, if you need to modify some of these variables (for instance, variables related to the country in which you are), use a MIB browser.

Provisioning Sequence

You can change the configuration at will after the initial provisioning and the provisioning system can refresh the AT-VP504E FXS configuration. The provisioning system consists of the Unit Manager and a DHCP server. The Unit Manager includes a provisioning client, provisioning server, and SNMP proxy server.

Restart Handler

The Provisioning Server provides a restart handler, which will synchronize the provisioned data in the AT-VP504E FXS in the event it goes off line and is rebooted again.

Changing Software Variables

Changing software variables involves contacting the proper MIB.

To change software variables:

1. Contact the AT-VP504E FXS with a MIB browser.

   You can use the built-in MIB browser of the Unit Manager. For more details, see the *IP Communication Server Administration* manual.

2. Open the proper MIB.

3. Select the specific variable you want to modify.

   All variables in the MIBs have a description as well as a list of possible values. Read the comments very carefully before changing a variable's value. The variables are subdivided in categories to facilitate your work.

4. Modify the variable according to the proper values listed.

5. Redo steps 3 and 4 for each variable you want to modify.

   Some variables will require to reboot the AT-VP504E FXS. The reboot will delete all statistics stored and will overwrite all volatile variable values in the MIBs.

Setting the Location (Country)

It is very important to set variables according to the country in which the AT-VP504E FXS is used because a number of parameter values are set according to this choice. These parameters are:

- Dial Tone
- Busy Tone
- Ringing Tone
- Special Information Tone
- Ring
- Impedance
- Tbrl-Impedance
- Line Attenuation (Input)
- Line Attenuation (Output)

For more information on these various country-specific settings, see "Appendix A - Country Specific Parameters" on page 119.

▶ To set a country location:

1. Locate the *countrySelection* variable in the *countryGroup* category of the Provisioning MIB.

   This variable indicates the current country used by the AT-VP504E FXS.

2. Set the variable as follows:
   - 0= Use Custom Configuration
   - 1= North America 1
   - 2= North America 2
   - 3= Austria
   - 4= France
   - 5= Germany 1
   - 6= Germany 2
   - 7= UK
   - 8= Italy
   - 9= Spain
   - 10 = Switzerland
   - 11 = Sweden
   - 12 = Australia
   - 13 = Japan
   - 14 = Israel

Note: When selecting the *Use Custom Configuration* option, the variables under the *portnDspCountrySpecificGroup* will be used. See the *MIB Reference Manual* for more details on these variables.

3. Set the *countryForceConfiguration* variable to **1** to override any custom configuration.

   Every custom configuration selection will be overridden by the selected country configuration in *countrySelection*.

4. Set the following variables:

Table 13: Country Variables

Variable	Description
countryCountryCode	Country code number associated to the current location of the AT-VP504E FXS.
countryAreaCode	Area Code number associated to the current location of the AT-VP504E FXS.

Example

Let's say your AT-VP504E FXS is located in Seattle, Washington. The Country settings would be as follows:

- **Country**: North America 1
- **Area Code**: 206

  This is the area code for the Seattle area.
- **Country Code**: 1

  This is the code indicating North American countries.

Overriding the Country-Specific Settings

You can instruct one or more port to ignore the default country-specific setting for a variable and rather use a custom value.

▶ **To override a country-specific variable value:**

1. Locate the *countryForceConfiguration* variable in the *countryGroup* of the Provisioning MIB.
2. Set the *countryForceConfiguration* variable to **0**.

Note: When selecting the *Use Custom Configuration* option, the variables under the *portnDspCountrySpecificGroup* will be used. See the *MIB Reference Manual* for more details on these variables.

Placing a Call

A call can be placed from a phone or fax connected to an AT-VP504E FXS unit. The unit automatically detects if the call originates from a voice transmission or fax transmission and acts accordingly.

When placing a call, the AT-VP504E FXS collects the DTMF digits dialed and sends a message to the Registrar Server (for instance, the IP Communication Server) or Call Agent. The Registrar Server or Call Agent sends back a list of contacts where the dialed number could be located.

For more information, please refer to the AT-VP504E FXS *User's Manual*.

4 Network Configuration

The AT-VP504E FXS uses a DHCP server to receive the IP addresses it needs to work properly. This chapter assumes that you know how to set up and use a DHCP server. If not, ask your network administrator to set up DHCP-related variables.

Setting the Speed of the Ethernet Connection

You can set the speed of the Ethernet connection of the AT-VP504E FXS.

▶ **To set the Ethernet connection speed:**

1. Contact the AT-VP504E FXS with a MIB browser.

   Be sure that you use the MIB files that match the version of the MIB located inside the current software build of the AT-VP504E FXS.

2. Locate the *interfaceEthernetSpeed* parameter (*InterfaceGroup* category) in the Provisioning MIB.

   This parameter sets the Ethernet connection at 10 Mb/s or 100 Mb/s. The following values are available:

   - 0 = Auto detect
   - 1 =10 Mb/s
   - 2 =100 Mb/s

   If unknown, set the variable to 0 so that the AT-VP504E FXS can auto detect the network speed.

3. Reboot the AT-VP504E FXS.

Using DHCP (Dynamic) or Static Configuration

The configuration your AT-VP504E FXS uses can either be:

- dynamically assigned (IP addresses assigned by a DHCP Server)
- static (static IP addresses defined in the Provisioning MIB)

Using DHCP (Dynamic) Configuration

Using DHCP-assigned IP addresses ensures that the AT-VP504E FXS receives the addresses that are stored in the DHCP server. See "Creating Vendor Specific Information" on page 39 for more details.

▶ To use DHCP configuration:

1. Locate the *interfaceUseDhcp* variable (*InterfaceGroup* category) in the Provisioning MIB.

   This variable indicates the origin of the configuration IP addresses.

2. Set the variable to **1, DHCP**.

   This is the default value.

3. Reboot the AT-VP504E FXS.

   The AT-VP504E FXS will not make a DHCP request in the following cases:

   - If all MIB variables *xxUseDhcp* are set to **0=False** at start-up.
   - If one of these variables is set to **1=True** after the initialization process.

   Table 14 lists the network variables that can be assigned via DHCP by using their vendor specific code.

Table 14: DHCP-Provided IP Addresses

IP Address	Description
Unit Manager	Uses the value via DHCP if *apaManagerUseDhcp* is set to **1**.
SIP User Agent Log	Uses the value via DHCP if *sipUALogUseDhcp* is set to **1**.
SIP Registrar Server	Uses the value via DHCP if *sipUAServerUseDhcp* is set to **1**.
SIP Proxy Server	Uses the value via DHCP if *sipUAServerUseDhcp* is set to **1**.
Syslog	Uses the value via DHCP if *syslogUseDhcp* is set to **1**.
TFTP Server	Uses the value via DHCP if *tftpUseDhcp* is set to **1**.
Emergency TFTP Server	Uses the value via DHCP if *tftpUseDhcp* is set to **1**.
SNTP Server	Uses the value via DHCP if *sntpUseDhcp* is set to **1**.

Each of these IP addresses has its own configurable vendor specific code. See "Creating Vendor Specific Information" on page 39 for more details.

Verifying the DHCP-Assigned IP Addresses

You can query the Provisioning MIB to see what are the IP addresses that have been assigned to the AT-VP504E FXS. Those IP addresses are located under the *interfaceDhcpGroup* of the Provisioning MIB in read-only variables.

Note: You can also see the DHCP server IP address in the read-only variable *interfaceDhcpServerIp*.

Using Static Configuration

Using static IP addresses allows you to bypass the DHCP or still be able to use the AT-VP504E FXS if you are not running a DHCP server.

▶ **To use Static configuration:**

1. Locate the *interfaceUseDhcp* variable (*InterfaceGroup* category) in the Provisioning MIB.

   This variable indicates the origin of the configuration IP addresses.

2. Set the variable to **0, Static**.

3. Locate the *interfaceStaticGroup* category.

   This category contains the IP addresses that you can set.

Table 15: IP Addresses to Set

IP Address	Variable
AT-VP504E FXS IP address	interfaceStaticLocalIp
Subnet Mask	interfaceStaticSubnetMaskIp
Default Router IP address	interfaceStaticDefaultRouterIp
Primary DNS IP address	interfaceStaticPrimDnsIp
Secondary DNS IP address	interfaceStaticSecDnsIp

4. Set the IP address of the above variables.

   Default IP addresses are already provided.

5. Reboot the AT-VP504E FXS.

Configuring the DHCP Server

DHCP servers generally allocate a range of IP addresses for use on a network and reserve IP addresses for specific devices using a unique identifier for each device. The AT-VP504E FXS unique identifier is its media access control (MAC) address. The MAC address appears on the label located on the bottom side of the unit (some previous versions may not have the MAC address on the label). It can also be found in the Provisioning MIB under the *interfaceMacAddress* variable. Allied Telesyn recommends that you reserve an IP address for each AT-VP504E FXS on the network.

In addition to the IP address, the DHCP server can set other configurable options within the AT-VP504E FXS, which expects to receive its network configuration and Unit Manager information from the DHCP server. These configuration options are called *vendor specific codes*.

Note: Allied Telesyn recommends that you use a Windows 2000- or Unix-based DHCP server. If you run Windows NT 4.0 and use the built-in Microsoft DHCP Server, you must use the Site Specific instead of Vendor Specific.

Connection to the DHCP Behavior

When the AT-VP504E FXS boots, it requests a DHCP offer to get its IP addresses and network variables. This offer is sent by the DHCP server with a *lease time*. The lease time is the time the offer from the DHCP is valid.

When making a request to the DHCP, the AT-VP504E FXS will send one (1) request every four (4) seconds for a maximum of five (5) retries, including the first one. As soon as one reply (or more) is received, the AT-VP504E FXS stops broadcasting. If the offer is valid, the AT-VP504E FXS takes it and continues its initialization procedure.

Note: If the *interfaceUseDhcp* variable is set to **0=False**, and any other *xxUseDhcp* variable (see Table 14 on page 36) is set to **1=True**, the AT-VP504E FXS will make its DHCP request with a lease time of 30 seconds that will not be renewed.

Network Configuration

Configure the DHCP server to set the following network options:

Table 16: Network Configuration

Option	Description	Type	Data Format	Example
Subnet Mask	Specifies subnet configuration	001	xxx.xxx.xxx.xxx	255.255.255.0
Routers	List of routers on your network	003	Array of IP Addresses	192.168.10.1 192.168.10.2
DNS Servers	List of DNS servers on your network	006	Array of IP Addresses	192.168.10.11 192.168.10.12

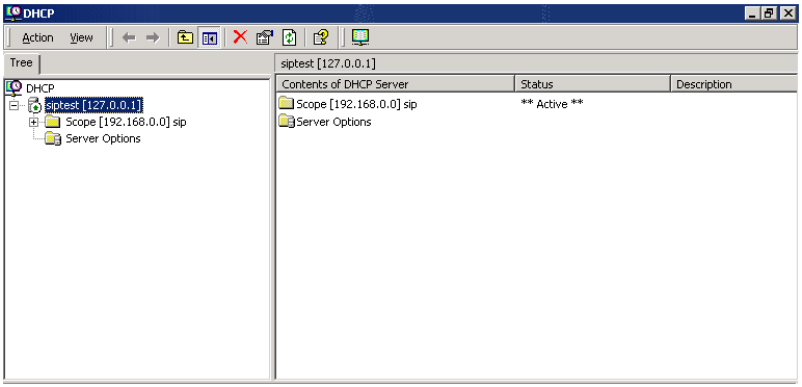
Creating Vendor Specific Information

The following section describes how to set Vendor specific information in a Windows 2000-based DHCP server. How to create vendor specific information differs from one DHCP server program to another.

▶ **To create vendor specific information:**

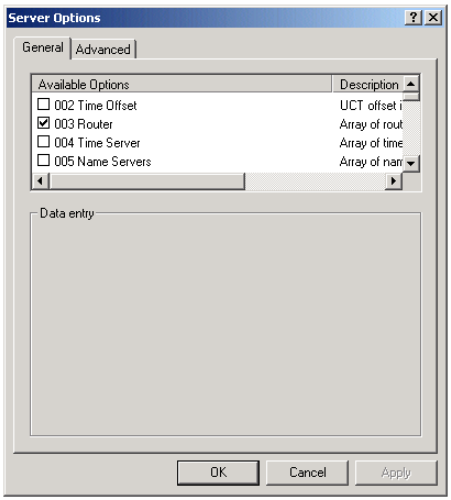
1. In *Start/Program/Administrative Tools*, select *DHCP*.
   The following window opens.

Figure 8: DHCP Manager



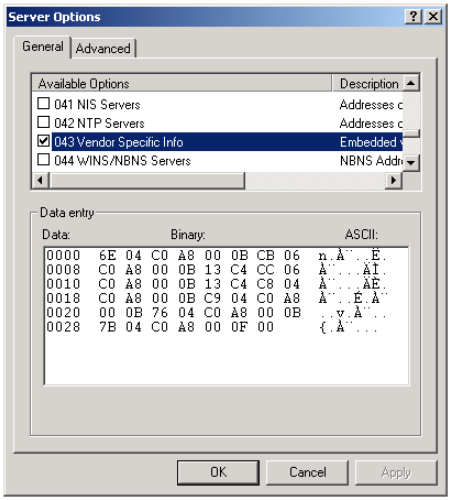
2. In the tree list on the left, select *Server Options*.
3. In the *Action* menu, select the *Configure Options* task.
   The following window opens:

Figure 9: Server Options Window



4. Scroll down the list and select the *043 Vendor Specific Info* option.

Figure 10: Vendor Specific Information



The *Server Options* window now lists the current Vendor Specific information set in the DHCP server.

5. Click in the last line entered, then type in the Vendor Specific Information you want to add.

   A new line will be automatically created. Use one line for each Vendor Specific information you want to add. You can enter a maximum of 255 characters per line.

   See "Entering IP Addresses" on page 41 for more details on the syntax to use.

6. When you are done, click *OK*.

Note: Firewall Information: the AT-VP504E FXS uses UDP port 5060.

Table 17 lists the Vendor specific information you can set in the DHCP server.

Table 17: Vendor Specific Codes

Information	MIB Variable	Code	Default	
			IP Address	Port #
Unit Manager	apaManagerDhcpVendorSpecificCode	200	192.168.0.10	162
SIP Logging	sipUALogDhcpVendorSpecificCode	202	192.168.0.10	6000
SIP Registrar Server	sipUAServerDhcpRegistrarVendorSpecificCode	203	192.168.0.10	5060
SIP Proxy Server	sipUAServerDhcpProxyVendorSpecificCode	204	192.168.0.10	5060
Syslog Daemon	syslogDhcpVendorSpecificCode	110	192.168.0.10	514
TFTP Server	tftpServerDhcpVendorSpecificCode	117	192.168.0.10	69
Emergency TFTP Server	tftpServerDhcpEmergencyVendorSpecificCode	118	192.168.0.10	69
SNTP Server	sntpDhcpVendorSpecificCode	208	192.168.0.10	123

Entering IP Addresses

There are two formats of address string:

- Long: Has a size of 6 hexadecimal characters and includes the IP address and port.

- Short: Has a size of 4 hexadecimal characters and includes only the IP address. In this case, the default port is used.

Table 18: Address String Formats

Variable	Valid Range	Typical Value	Note
IP Address	Any valid IP address	192.168.0.2	N/A
Port	1 - 32,768	162	Not present in the format with dimension 4.

If the DHCP request fails or the address is not in the vendor specific codes, the following applies:

1. If the DHCP value already in the MIB is valid, it is kept.
2. If not, the static value is used if valid.
3. If not, the default value is used.

Example

The following example shows how to enter the Syslog IP address 192.168.0.10 (with the default port used) and the same address at port 2545. The format is in hexadecimal.

Figure 11: Example – Short Address String

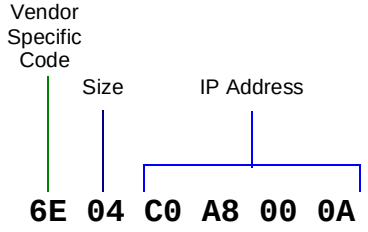
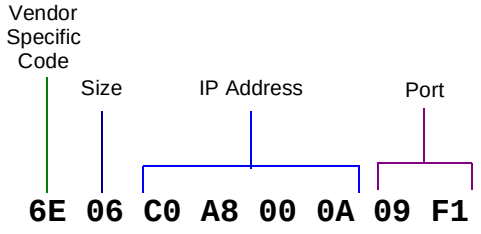


Figure 12: Example – Long Address String



5 Software Download

This chapter describes how to download the latest software version available on the designated software server into the AT-VP504E FXS. It also describes how to update the rescue application that automatically starts in case of software download problems.

Before Downloading

To download a new software, you must setup the following applications on your computer:

- TFTP server
- MIB browser (with the current AT-VP504E FXS MIB tree)

  You can use the user interface of the IP Communication Server. See the *IP Communication Server Administration Manual* for more details.
- Syslog daemon (optional)

Configuring the TFTP Server

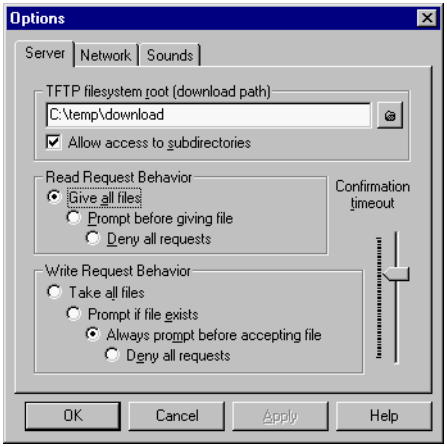
Downloading a new software version into the AT-VP504E FXS requires a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the software file server.

If you don't have a TFTP server, you can install "PumpKIN" (one of the best and fastest TFTP servers available). PumpKIN is located on the documentation CD provided with your AT-VP504E FXS communication unit.

▶ **To configure the PumpKIN TFTP server:**

1. Install the TFTP application on the PC designated as the software file server and run it.
2. From the main screen of PumpKIN, go into the *Options* menu and configure the path of the new *.bin* application file location.
3. Select *Give all files* from the *Read Request Behavior* section, then click *OK*. Leave the application running.

Figure 13: PumpKIN Options



4. Set the following variables in the *tftpGroup* category of the Provisioning MIB.

Table 19: TFTP Settings

Variable	Description
tftpFileName	VP500 communication unit file name to download from the TFTP Server. **Default Value**: apa.bin
tftpEmergencyFileName	Emergency VP500 communication unit file name to download when the Rescue application starts. **Default Value**: apa_emergency.bin
tftpTimeOut	Connection time-out value. **Default Value**: 30
tftpBlockSize	Default block size. **Default Value**: 1024
tftpDownloadStatus	Read-only parameter that gives the status of the download process.

DHCP vs. Static Configuration

The TFTP server information can be assigned through a DHCP server or set statically.

▶ **To use DHCP-assigned information:**

1. Locate the *tftpUseDhcp* variable (under *tftpGroup*).

   This variable defines whether the AT-VP504E FXS must ask for its TFTP server settings through a DHCP server or not.

2. Set the *tftpUseDhcp* variable to **1=DHCP**.

   You can query the TFTP server's IP address and Port number assigned by the DHCP server in the following read-only variables:

   - tftpServerDhcpHost
   - tftpServerDhcpPort
   - tftpServerDhcpEmergencyHost
   - tftpServerDhcpEmergencyPort

3. Set the DHCP Vendor Specific code of the TFTP server in the *tftpServerDhcpVendorSpecificCode* variable.

   This code can be any number between 0 and 254. The default value is **201**.

4. Set the DHCP Vendor Specific code of the TFTP emergency server in the *tftpServerDhcpEmergencyVendorSpecificCode* variable.

   This code can be any number between 0 and 254. The default value is **118**.

▶ **To use static information:**

1. Locate the *tftpUseDhcp* variable (under *tftpGroup*).

   This variable defines whether the AT-VP504E FXS must ask for its TFTP server settings through a DHCP server or not.

2. Set the *tftpUseDhcp* variable to **0=Static**.

3. Set the following variables:

Table 20: TFTP Static Address

Variable	Description
tftpServerStaticHost	Static TFTP server IP address or domain name. **Default Value**: 192.168.0.10
tftpServerStaticPort	Static TFTP server IP Port number. **Default Value**: 69
tftpServerStaticEmergencyHost	Static emergency TFTP server IP address or domain name. **Default Value**: 192.168.0.10
tftpServerStaticEmergencyPort	Static emergency TFTP server IP Port number. **Default Value**: 514

Download Procedure

When upgrading the software in the AT-VP504E FXS to a new protocol or a new major revision, Allied Telesyn recommends to re-create the file system of the AT-VP504E FXS. To do this, you must perform a Factory Default Settings procedure. See “Factory Settings Mode” on page 24 for more details.

▶ **To download the latest software:**

1. Make sure you are trying to install the latest version of the software.

2. Setup the TFTP server that will be used to download the software (see “Configuring the TFTP Server” on page 43).

3. Contact the AT-VP504E FXS with any SNMP MIB browser.

   Be sure to use the MIB modules that match the version of the MIBs located inside the current software build of the AT-VP504E FXS.

4. Locate the *tftpGroup* category in the Provisioning MIB.

   This category contains all the variables you must set to properly download a software version. These variables include:

   - Binary file name to download
   - Software server address where to get the binary file
   - Port number of the software server

   This can be done statically through SNMP, automatically through the Unit Manager, or dynamically through the DHCP server.

5. If the DHCP server did not provide the information to the AT-VP504E FXS, configure the *tftpServerStaticHost* variable in the *tftpGroup* category with the current address of the PC that runs the TFTP server.

   For example, set the variable with a valid IP address such as 192.168.0.2.

6. Configure the *tftpFileName* variable with the current name of the software that will be downloaded into the AT-VP504E FXS.

   You can use any name you want. However, make sure that the name you enter matches the name of the file located on the TFTP server.

7. Disable the AT-VP504E FXS by setting the *apaCmdMode* variable to **1**.

8. Initiate the image download by setting the *apaCmdDownload Software* variable to **1**.

   This will start the download process.

9. Query the *tftpDownloadStatus* variable and see if it is reset to **1**. If yes, then the update is done.

Warning: Never shutdown the AT-VP504E FXS manually while in the In Progress state of the image download process, because the image may be partially written to the EEPROM and the AT-VP504E FXS will be unable to restart.

If you are using a Syslog daemon, you will receive messages that inform you when the update is completed and that you can now reboot the AT-VP504E FXS. The LEDs will also indicate the completion of the download process. See "LED States" on page 48 for more details.

The AT-VP504E FXS will stop responding for a few seconds while the image is written to the EEPROM memory. This is normal and it may take 20 to 30 seconds before the AT-VP504E FXS comes back and starts responding again.

10. Reboot the AT-VP504E FXS so the new image can take effect.

11. Update the MIB browser with the latest MIB version coming with the download.

LED States

When the AT-VP504E FXS initiates a software download, the three LEDs located on the front panel are used to report the status of the process:

Table 21: LED States in Software Download

Event	LED State
IMAGE_DOWNLOADING (download phase)	Each LED blinks alternately.
IMAGE_WRITING (writing to EEPROM phase)	*Test* LED ON, *LAN* LED ON, *Power* LED OFF. **Note**: Do not turn the AT-VP504E FXS off while in this state.
IMAGE_UPDATE_FAIL	All LEDs blink at the same time.
IMAGE_UPDATE_SUCCESS	All LEDs ON.

Emergency Software Procedure

Once the new software file is successfully downloaded into the RAM of the AT-VP504E FXS, this file is transferred from the RAM to the EEPROM. The AT-VP504E FXS then reboots. If the transfer from the RAM to the EEPROM is suddenly interrupted, only a part of the software file is transferred to the EEPROM. Without any protection against this situation, the software file in the EEPROM is incomplete and the AT-VP504E FXS is not functional.

A transfer may be interrupted for the following reasons:

- An electrical shortage can interrupt the transfer of the software file from the RAM to the EEPROM.
- The user of the AT-VP504E FXS can accidentally power off the unit when the software file is being transferred from the RAM to the EEPROM.

To avoid this situation, the AT-VP504E FXS emergency software procedure (also called rescue application) automatically starts a new software download.

Downloading the Emergency Software

You must download the latest emergency software into the AT-VP504E FXS.

To download the latest emergency software (rescue application):

1. Setup the TFTP server that will be used to download the software (see "Configuring the TFTP Server" on page 43).
2. Contact the AT-VP504E FXS with any SNMP MIB browser.

   Be sure to use the MIB modules that match the version of the MIBs located inside the current software build of the AT-VP504E FXS.
3. Locate the *tftpGroup* category in the Provisioning MIB.

   This category contains all the variables you must set to properly download a software version. These variables include:

   - Binary file name to download
   - Software server address where to get the binary file
   - Port number of the software server

   This can be done statically through SNMP, automatically through the Unit Manager, or dynamically through the DHCP server.

4. If the DHCP server did not provide the information to the AT-VP504E FXS, configure the *tftpServerEmergencyStaticHost* variable in the *tftpGroup* category with the current address of the PC that runs the TFTP server.

   For example, set the variable with a valid IP address such as 192.168.0.2.

5. Configure the *tftpEmergencyFileName* variable with the current name of the emergency software that will be downloaded into the AT-VP504E FXS.

   You can use any name you want. However, make sure that the name you enter matches the name of the file located on the TFTP server.

6. Disable the AT-VP504E FXS by setting the *apaCmdMode* variable to **1**.

7. Initiate the image download by setting the *apaCmdDownload Software* variable to **1**.

   This will start the download process.

8. Query the *tftpDownloadStatus* variable and see if it is reset to **1**. If yes, then the update is done.

Warning: Never shutdown the AT-VP504E FXS manually while in the In Progress state of the image download process, because the image may be partially written to the EEPROM and the AT-VP504E FXS will be unable to restart.

If you are using a Syslog Daemon, you will receive messages that inform you when the update is completed and that you can now reboot the AT-VP504E FXS. The LEDs will also indicate the completion of the download process. See "LED States" on page 48 for more details.

The AT-VP504E FXS will stop responding for a few seconds while the image is written to the EEPROM memory. This is normal and it may take 20 to 30 seconds before the AT-VP504E FXS comes back and starts responding again.

9. Reboot the AT-VP504E FXS so the new image can take effect.

Using the Emergency Software

When the emergency software procedure starts, the following steps apply:

1. The AT-VP504E FXS tries to initiate the software download with the primary software server.
2. If the software download fails with the primary software server, the AT-VP504E FXS tries to initiate the software download with the secondary software server.
3. If the software download also fails with the secondary software server, the AT-VP504E FXS idles for one (1) minute.
4. After this one (1) minute, the AT-VP504E FXS retries to initiate the software download.
5. If the software download fails again with the primary and secondary software server, the AT-VP504E FXS idles for two (2) minutes before trying to initiate the software download.
6. If the emergency software download still fails, the AT-VP504E FXS retries to initiate the software download by doubling the delay between each try up to a maximum of 16 minutes:
    - first try: 1 minute delay
    - second try: 2 minutes delay
    - third try: 4 minutes delay
    - fourth try: 8 minutes delay
    - fifth try: 16 minutes delay
    - sixth try: 16 minutes delay
    - etc.

    The emergency software procedure will continue until the software download completes successfully. The software download can fail if the software server cannot be reached or if the software file is not found on the software server.

6 System Failure Bypass Connector Configuration

The AT-VP504E FXS has a fifth RJ-11 connector used to connect to a standard SCN line, called *Bypass*. In the event of a commercial power failure or network failure, this feature permits users to make and receive calls even when the AT-VP504E FXS is not operating.

System Failure Bypass Connector Settings

During normal operation, the SCN line connected to the *Bypass* port is switched out of the circuit through commuting relays. When power is removed from the AT-VP504E FXS, the relay setting is restored to a connected state and the SCN line can be used as an emergency line. Consequently, a phone/fax used on FXS **Port 1** will be directly connected to this SCN line.

When the error conditions have been cleared or the power is restored, Port 1 stays in System Failure Bypass connection until the device connected to it is on-hook. This safety feature ensures that an emergency call does not get disconnected from the SCN.

Setting the Bypass Service

The following parameters can be set:

Table 22: Bypass Connector Settings

Variable	Description
apaByPassModeAlways Enable variable set to **1**	Always activate System Failure Bypass service. The System Failure Bypass is unconditionally activated.
apaByPassModeLanFail Enable variable set to **1**	Activate System Failure Bypass service when Ethernet connection is lost. The System Failure Bypass is activated when: • Network is down. • Network connection is recovered but a System Failure Bypass call is still in progress.
apaByPassModeServer FailEnable set to **1**	Activate System Failure Bypass service when: • The server is down. • The server is back on-line but a System Failure Bypass call is still in progress.

Note: The *apaByPassModeAlwaysEnable* variable and the following two exclude each other. The *apaByPassModeLanFailEnable* and *apaByPassModeServerFailEnable* variables can be simultaneously active.

All four ports of the AT-VP504E FXS must be properly enabled and set in order to work as they should be.

When a telephone connected to one of the AT-VP504E FXS FXS ports is put on-hook, the AT-VP504E FXS signals this by performing a current loop drop. The current loop drop, also referred to Power Denial mode by some manufacturers, is typically used for disconnect supervision. It signals that the remote telephone has been taken on-hook. The AT-VP504E FXS will detect a Current Drop if this signal is maintained for at least 600 ms with an open circuit or has a current drop lower than 0.4 mA.

Enabling Ports

You can independently enable/disable each port of the AT-VP504E FXS.

▶ **To set basic port properties:**

1. Locate the *port1Enable* variable (under *port1Grou*p).

   This variable enables/disables port #1 of the AT-VP504E FXS.

2. Set the *port1Enable* variable to **1=Enable**.

   The AT-VP504E FXS cancels the port registration to the SIP server when the port is disabled and registers it when the port is enabled.

Setting Basic DSP Variables

DSP (Digital Signal Processing) variables define how to transmit the audio/data signal.

▶ **To set basic DSP variables:**

1. Locate the *port1DspGroup* category.

2. Define *Jitter Buffer* variables.

   The jitter buffer allows better protection against packet loss, but increases the voice delay. If the network to which the AT-VP504E FXS is connected suffers from a high level of congestion, the level of jitter buffer protection should be

higher. If the network to which the AT-VP504E FXS is connected suffers from a low level of congestion, the level of jitter buffer protection should be lower.

Table 23: Jitter Buffer Variables

Variable	Definition
port1DspMaxJitterBufferLen	Maximum jitter buffer length in ms. **Default Value**: 300
port1DspTargetJitterBufferLen	Target jitter buffer length in ms. **Default Value**: 150
port1DspAdaptativityJitterBuffer	Adaptative Jitter Buffer. • 0 =OFF • 1 =ON

3. Define the *port1DspVoiceActivityDetection* variable.

   The Voice Activity Detection (VAD) enables the AT-VP504E FXS to detect when the user talks, thus avoiding to send silent RTP packets. This saves on network resources. However, the VAD may affect packets that are not really silent (for instance, cut sounds that are too low). The VAD can thus lightly affect the voice quality.

Table 24: Voice Activity Detection Variables

Variable	Description
0 = Off	VAD is not used.
1 = Transparent	Silences are least detected, affects the voice quality the least.
2 = Conservative	Silence detection is medium, voice quality affected is medium.

The difference between transparent and conservative is how "aggressive" the algorithm will consider something as an inactive voice and how "fast" it will stop the voice stream. A setting of conservative is a little bit more agressive compared to a setting of transparent to react to silence.

The default value is **2 = Conservative**.

4. Define the *port1DspEchoCancelControl* variable.

   The Echo cancel control allows to cancel the echo effect caused by signal reflections. Available values are:

   - 0 =OFF
   - 1 =ON

Note: You can repeat the same process for each port of the AT-VP504E FXS.

Setting User Gain Variables

The user gain allows the user to modify the input and output sound level.

Warning: Use these settings with great care, because there are no limits to the sound level range you can use.

Using a high user gain may cause sound saturation (the sound is distorted). These parameters also directly affect the fax communication quality and may even prevent a fax to be sent.

The user gain may be used to compensate if there is no available configuration for the country in which the AT-VP504E FXS is located.

▶ **To set User gain variables:**

1. Locate the *port1DspUserGainGroup* category.
2. Define the following variables:

Table 25: User Gain Variables

Variable	Description
port1DspUserGainInputOffset	User input gain offset in dB. Values range from -255 dB to +255 dB. The value may also be decimal (e.g. -5.5 dB). **Default Value**: 0
port1DspUserGainOutputOffset	User output gain offset in dB. Values range from -255 dB to +255 dB. The value may also be decimal (e.g. -5.5 dB). **Default Value**: 0

Note: You can repeat the same process for each port of the AT-VP504E FXS.

Setting Country-Specific Variables

The variables in the *port1DspCountrySpecificGroup* category can change in different countries, so they need to be set according to the AT-VP504E FXS location.

Table 26: Country-Specific Variables

Variable	Description
port1DspCountrySpecificGainConfiguration	Select the configuration to use. • 0 = Use custom configuration • 1 = Use default country configuration **Default Value**: 1
port1DspCountrySpecificGainBaseInput	Country specific base input gain. **Default Value**: 3648
port1DspCountrySpecificGainBaseOutput	Country specific base output gain. **Default Value**: 3029
port1DspCountrySpecificGainBaseInputOffset	Country specific base input gain offset in dB. **Default Value**: 0
port1DspCountrySpecificGainBaseOutputOffset	Country specific base output gain offset in dB. **Default Value**: 0

Note: You can repeat the same process for each port of the AT-VP504E FXS.

Selecting the Preferred Codec

The AT-VP504E FXS supports various codecs for transmitting audio or data signals.You must set and enable these codecs for **each** port.

▶ **To select a codec:**

1. Locate the *port1DspPreferredCodec* variable (under *port1DspCodecGrou*p).

   This variable sets the preferred codec for this port.

2. Select one of the available configurations:
   - 0= G.711 u-Law (PCMU)
   - 1 = G.711 a-Law (PCMA)
   - 2 = G.723.1
   - 3 = G.729.AB

   The default value is **0 = G.711 u-Law**.

Enabling Individual Codecs

Codecs are enabled by setting the variable to **1 =Enable**. The following codec variables are available:

- port1DspCodecG711aLawEnable
- port1DspCodecG711uLawEnable
- port1DspCodecG7231Enable
- port1DspCodecG729ABEnable
- port1DspCodecT38Enable

Table 27 lists other codec options that can be set.

Table 27: Other Codec Options

Variable	Definition	Values
port1DspCodecG711aLawPTimeMax	Maximum Packetization time in ms.	10-80
port1DspCodecG711uLawPTimeMax	Maximum Packetization time in ms.	10-80
port1DspCodecG7231PTimeMax	Maximum Packetization time in ms.	30
port1DspCodecG729APTimeMax	Maximum Packetization time in ms.	20-40
port1DspCodecG711aLawPTimeMin	Minimum Packetization time in ms.	10-80
port1DspCodecG711uLawPTimeMin	Minimum Packetization time in ms.	10-80
port1DspCodecG7231PTimeMin	Minimum Packetization time in ms.	30

Table 27: Other Codec Options (Continued)

Variable	Definition	Values
port1DspCodecG729APTimeMin	Minimum Packetization time in ms.	20-40
port1DspCodecG7231BaudRate	Baud Rate Value.	5.3 or 6.3 kbps

Note: You can repeat the same process for each port of the AT-VP504E FXS.

8 Unit Manager Configuration

The Unit Manager is a module of the IP Communication Server or the Unit Manager Network product. Both are used to remotely configure VP500 communication units. The Unit Manager is a graphical interface that helps you work with the MIB variables involved in the AT-VP504E FXS setup.

Using the Unit Manager

You have the choice of setting up AT-VP504E FXS communication units directly with a SNMP browser or use the Unit Manager to remotely set up units.

Note: For more information on how to use the Unit Manager to set up AT-VP504E FXS communication units, please refer to the IP Communication Server manual.

▶ **To use the Unit Manager:**

1. Locate the *apaManagerEnable* variable (under *apaManagerGroup*).

   This variable enables the Unit Manager to remotely manage the AT-VP504E FXS.

2. Set the *apaManagerEnable* variable to **1=Enable**.

3. Set the Trap retransmission period to the desired value.

   The default value is 60 seconds.

4. Set the Trap retransmission retry count to the desired value.

   When the retry count is elapsed, the AT-VP504E FXS will stop the provisioning sequence. The default value is 10.

   If this variable is set to -1, then the provisioning sequence will never be stopped. The trap will be sent until the Unit Manager replies.

DHCP vs. Static Configuration

Unit Manager information such as its IP address and port number can be assigned through a DHCP server or set statically.

▶ **To use DHCP-assigned information:**

1. Locate the *apaManagerUseDhcp* variable (under *apaManagerGroup*).

   This variable defines whether the AT-VP504E FXS must get its Unit Manager configuration through a DHCP server or not.

2. Set the *apaManagerUseDhcp* variable to **1=DHCP**.

   You can query the Unit Manager's IP address and Port number assigned by the DHCP server in the *apaManager DhcpPrimHost* and *apaManagerDhcpPrimTrapPort* read-only variables.

3. Set the DHCP Vendor Specific code of the Unit Manager in the *apaManagerDhcpVendorSpecificCode* variable.

   This code can be any number between 0 and 254. The default value is **200**.

▶ **To use static information:**

1. Locate the *apaManagerUseDhcp* variable (under *apaManagerGroup*).

   This variable defines whether the AT-VP504E FXS must get its Unit Manager configuration through a DHCP server or not.

2. Set the *apaManagerUseDhcp* variable to **0=Static**.

3. Set the following variables:

Table 28: Unit Manager Static Address

Variable	Description
apaManagerStaticPrimHost	Static Unit Manager IP address or domain name. **Default Value**: 192.168.0.10
apaManagerStaticPrimTrapPort	Static Unit Manager IP port number. **Default Value**: 162

9 Miscellaneous Configuration

This chapter describes other configuration settings not covered in the previous chapters.

Using QoS

QoS (Quality of Service) features enable network managers to decide on packet priority queuing. The AT-VP504E FXS supports the Differentiated Services (DS) field and 802.1q taggings. There are two variables – one variable for media (T.38, RTP, etc.) and one for signalling (SIP).

Note: The AT-VP504E FXS does not support RSVP (Resource Reservation Protocol).

Differentiated Services (DS) Field

You can set various DIfferentiated Services parameters that will allow you to control the network traffic.

What are Differentiated Services?

Differentiated Services (DiffServ, or DS) is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence – for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic.

Unlike the earlier mechanisms of 802.1p tagging and Type of Service (ToS), Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet. An analogy is made to travel services, in which a person can choose among different modes of travel – train, bus, airplane – degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth.

For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors – known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (Internet Protocol) header specifies the per hop behavior for a given flow of packets. The DS field structure is presented below:

```
        0   1   2   3   4   5   6   7
        +---+---+---+---+---+---+---+---+
        | DSCP                  |  CU   |
        +---+---+---+---+---+---+---+---+
```

- *DSCP*: Differentiated Services CodePoint.
- *CU*: Currently Unused. The CU bits should always be set to 0.

For both signalling and media packets, the DSCP field is configurable independently. For future extensibility, the entire DS field (TOS byte) will be configurable.

Note: It is the network administrator's responsibility to provision the AT-VP504E FXS with standard and correct values.

▶ To enable the DS field configuration:

1. Locate the following attributes under the *interfaceQoSGroup* of the Provisioning MIB:
   - interfaceQoSSignalingDSFieldValue
   - interfaceQoSMediaDSFieldValue

   These variables are 1 octet scalar ranging from 0 to 255. The DSCP default value should be 101110 for both signalling and media packets. This results in the DS field value of: 10111000 (184d).

   This default value would result in a value of “101” precedence bits, low delay, high throughput, and normal reliability in the legacy IP networks (RFC 791, RFC 1812). Network managers of legacy IP networks could use the above-mentioned values to define filters on their routers to take advantage of priority queuing. The default value is based on the Expedited Forwarding PHB (RFC 2598) recommendation.

2. Set the value you want to use.

   You can find references on DS field under the IETF working group DiffServ.

   For more information, please refer to the following RFC documents and the *MIB Reference* manual:
   - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (RFC 2474)
   - An Architecture for Differentiated Services (RFC 2475)
   - Assured Forwarding PHB Group (RFC 2597)
   - An Expedited Forwarding PHB (RFC 2598)

IEEE 802.1q The 802.1q standard recommends the use of the 802.1q VLAN tags for Ethernet frames traffic prioritization. VLAN tags are 4-byte headers in which three bits are reserved for priority indication. The values of the priority bits must be provisioned.

Note: It is the network administrator's responsibility to provision the AT-VP504E FXS with standard and correct values.

▶ **To enable the IEEE 802.1q user priority configuration:**

1. Locate the following attributes under the *interfaceQoSGroup* of the Provisioning MIB:
   - interfaceQoSSignalingIeee8021QFilterEnable
   - interfaceQoSMediaIeee8021QFilterEnable

Note on the Implementation of the IEEE Standard 802.1q

This note applies only for previous hardware revisions that do not use revision D of the main CPU, the Motorola PowerPC 860.

The implementation of the IEEE Standard 802.1q in the AT-VP504E FXS has a minor problem due to hardware limitations.

802.1q increases the Ethernet frame header by 4 bytes, adding a Virtual LAN ID and a user_priority. This is useful to limit broadcasts that cross bridges, and it may also prioritize frames in the queuing algorithm of switches. However, it also increases the maximum possible size of Ethernet frames from 1518 to 1522 bytes, and this might not be handled adequately by every hardware.

A workaround is available for PCs running Windows to avoid sending 1522 bytes packets (note that this happens only in special and rare cases). The workaround is to reduce the MTU of the interface (the one that sends packets with 802.1q framing) by 4 bytes.

- Use the registry editor (regedt32 on Windows 2000) and go to the key:

  ```
  \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<ethernet adapter>\Parameters\Tcpip
  ```

  where <Ethernet adapter> can be found by using the command “ipconfig /all”.
- Add (or modify) a value named MTU of type REG_DWORD. Set it to 1496 (instead of 1500), in decimal. Reboot the computer to have those changes in effect.
- To validate that your changes are correct, try to ping the AT-VP504E FXS with large packets once rebooted:

  ```
  ping -l 2000
  ```

This will cause IP fragmentation, the first fragment being as large as the interface allows it. With the MTU reduced, you should now receive an answer. You can even ping with packets of 65500 bytes!

2. Set the value of these parameters to **1 = Enable**.

   The corresponding user priority configuration is enabled.

3. Locate the following attributes under the *interfaceQoSGroup* of the Provisioning MIB:
   - interfaceQoSSignalingIeee8021QUserPriority
   - interfaceQoSMediaIeee8021QUserPriority

   These attributes are 1 octet scalar ranging from 0 to 7. The 802.1q default priority value should be 6 for both signaling and media packets.

For more information, please refer to the *MIB Reference* manual.

VLAN You can set various VLAN parameters that will allow you to control user priority.

VLANs

VLANs are created with standard Layer 2 Ethernet. A VLAN Identifier (VID) is associated with each VLAN. VLANs aim to offer the following benefits:

- VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.
- VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of moves, adds, and changes in members of these groups.
- Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.
- As far as possible, VLANs maintain compatibility with existing bridges and end stations.

The VLAN field in the Ethernet file is located after both destination and source addresses:

```
         0                   1
         0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7   (byte)
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        | Dest Addr | Src Addr  | VLAN  | Type/Length | ...
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The VLAN field is separated as follows:

```
        0  (bit)            1                   2                   3
         0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |             0x8100            | Pri |T|          VID          |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

For both signalling and media packets, the VLAN priority section is configurable independently.

▶ **To enable the VLAN configuration:**

1. Locate the *interfaceVlanIeee8021QTaggingEnable* attribute under the *interfaceVlanGroup* of the Provisioning MIB.
2. Set the value of this parameter to **1 = Enable**.

   The VLAN configuration is enabled.
3. Locate the following attributes under the *interfaceVlanGroup* of the Provisioning MIB:
   - interfaceVlanIeee8021QVirtualLanID
   - interfaceVlanIeee8021QDefaultUserPriority
4. Set the value of these attributes.

For more information, please refer to the *MIB Reference* manual.

Syslog Daemon Configuration

The AT-VP504E FXS can send administrative messages to the Syslog daemon, which is a tool you can use to monitor events in the AT-VP504E FXS. If no Syslog daemon address is provided by a DHCP server or specified by the administrator, no messages are sent.

Why a Syslog Daemon?

The Syslog daemon is a general purpose utility for monitoring applications and network devices with the TCP/IP protocol. With this software, you can monitor useful messages coming from your AT-VP504E FXS communication unit.

For example, if you want to download a new software into the AT-VP504E FXS, you can monitor each step of the software download phase. Furthermore, if the unit encounters an abnormal behaviour, you can sometimes see accurate messages that will help you troubleshoot the problem.

▶ **To enable the Syslog daemon:**

1. Locate the *syslogMsgEnable* variable (under *syslogGrou*p).

   This variable enables the syslog daemon messages.
2. Set the *syslogMsgEnable* variable to **1=Enable**.
3. Select a tracing mask option in the *syslogTracingMask* variable.

   Available values are:
   - 0 = Absolutely no Tracing

- 1 = Critical errors
- 2 = Error conditions
- 3 = Warning conditions
- 4 = Informational messages
- 5 = Debug-level messages (use with care)

Higher level mask includes lower level masks, e.g.: Error conditions (2) include Critical errors (1).

The default value is **4 = Informational messages**.

DHCP vs. Static Configuration

The Syslog daemon information can be assigned through a DHCP server or set statically.

▶ **To use DHCP-assigned information:**

1. Locate the *syslogUseDhcp* variable (under *syslogGroup*).

   This variable defines whether the AT-VP504E FXS must ask for its Syslog daemon settings through a DHCP server or not.

2. Set the *syslogUseDhcp* variable to **1=DHCP**.

   You can query the Syslog daemon's IP address and port number assigned by the DHCP server in the *syslogDhcpHost* and *syslogDhcpPort* read-only variables.

3. Set the DHCP Vendor Specific code of the Syslog daemon in the *syslogDhcpVendorSpecificCode* variable.

   This code can be any number between 0 and 254. The default value is **110**.

▶ **To use static information:**

1. Locate the *syslogUseDhcp* variable (under *syslogGroup*).

   This variable defines whether the AT-VP504E FXS must ask for its Syslog daemon settings through a DHCP server or not.

2. Set the *syslogUseDhcp* variable to **0=Static**.

3. Set the following variables:

Table 29: Syslog Daemon Static Address

Variable	Description
syslogStaticHost	Syslog server static IP address or domain name. **Default Value**: 192.168.0.10
syslogStaticPort	Syslog server static IP port number. **Default Value**: 514

Configuring the Syslog Daemon

You must configure both your AT-VP504E FXS communication unit to send Syslog messages and your Syslog daemon to capture those messages.

▶ **To configure your AT-VP504E FXS:**

1. Go to the Unit Manager and enter the level of messages you want your AT-VP504E FXS to send.
2. Enter the IP address of the computer on which the Syslog Daemon is running.

   For more information, see your *IP Communication Server Administration Manual*.

▶ **To enable your Syslog daemon to capture your AT-VP504E FXS messages:**

1. Refer to your Syslog daemon's documentation to learn how to properly configure it to capture messages.

SNMP Configuration

The SNMP Group parameters allow you to set information pertaining to the SNMP protocol

Table 30: SNMP Configuration Variables

Variable	Description
snmpAgentPort	SNMP Agent port number on which the unit must listen for SNMP requests. **Default Value**: 161

Table 30: SNMP Configuration Variables (Continued)

Variable	Description
snmpSystem Description	A textual description of the unit. This should include the full name and version identification of the system's hardware type, software operating system, and networking software.
snmpSystemObjectID	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining "what kind of box" is being managed. For example, if vendor "Flintstones, Inc." was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its "Fred Router". **Default Value**: 43.6.1.4.1.4935.1.1.1.1.1
snmpSystemContact	The textual identification of the contact person for this managed node, along with information on how to contact this person. If no contact information is known, the value is the zero-length string.
snmpSystemName	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. **Default Value**: UNIT
snmpSystemLocation	The physical location of this node (e.g., "telephone closet, 3rd floor"). If the location is unknown, the value is the zero-length string.

Table 30: SNMP Configuration Variables (Continued)

Variable	Description
snmpSystem Description	A textual description of the unit. This should include the full name and version identification of the system's hardware type, software operating system, and networking software.
snmpSystemObjectID	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining "what kind of box" is being managed. For example, if vendor "Flintstones, Inc." was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its "Fred Router". **Default Value**: 43.6.1.4.1.4935.1.1.1.1.1
snmpSystemContact	The textual identification of the contact person for this managed node, along with information on how to contact this person. If no contact information is known, the value is the zero-length string.
snmpSystemName	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. **Default Value**: UNIT
snmpSystemLocation	The physical location of this node (e.g., "telephone closet, 3rd floor"). If the location is unknown, the value is the zero-length string.

Table 30: SNMP Configuration Variables (Continued)

Variable	Description
snmpSystemService	A value which indicates the set of services that this entity may potentially offer. The value is a sum. This sum initially takes the value zero. Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs only routing functions would have a value of 4 ($2^{(3-1)}$). In contrast, a node which is a host offering application services would have a value of 72 ($2^{(4-1)} + 2^{(7-1)}$). Note that in the context of the Internet suite of protocols, values should be calculated accordingly: layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., supports the IP) 4 end-to-end (e.g., supports the TCP) 7 applications (e.g., supports the SMTP) For systems including OSI protocols, layers 5 and 6 may also be calculated. **Default Value**:72

SNTP Settings

The Simple Network Time Protocol (SNTP)[1] enables the notion of time (date, month, time) into the AT-VP504E FXS. It is especially required when dealing with features such as the Caller ID.

SNTP is used to synchronize a SNTP client with a SNTP or NTP server by using UDP as transport (see RFC 1769 for more details).

▶ **To enable the SNTP feature:**

1. Locate the *sntpEnable* variable (under *sntpGroup*).
   This variable enables the SNTP feature.
2. Set the *sntpEnable* variable to **1=Enable**.

1. Only available in units that run the SIP signalling protocol.

3. Set the following synchronization information:

Table 31: SNTP Synchronization Information

Variable	Description
sntpSynchronization Period	Interval, in minutes, before sending a SNTP time request to the SNTP server. Available values are between 1 and 1440 minutes. **Default Value**: 1140
sntpSynchronization PeriodOnError	Interval, in minutes, before sending a SNTP time request to the SNTP server after a SNTP error. Available values are between 1 and 1440 minutes. **Default Value**: 1140

DHCP vs. Static Configuration

The SNTP server information can be assigned through a DHCP server or set statically.

▶ **To use DHCP-assigned information:**

1. Locate the *sntpUseDhcp* variable (under *sntpGroup*).

   This variable defines whether the AT-VP504E FXS must ask for its SNTP server settings through a DHCP server or not.

2. Set the *sntpUseDhcp* variable to **1=DHCP**.

   You can query the SNTP server's IP address and port number assigned by the DHCP server in the *sntpDhcpHost* and *sntpDhcpPort* read-only variables.

3. Set the DHCP Vendor Specific code of the SNTP feature in the *sntpDhcpVendorSpecificCode* variable.

   This code can be any number between 0 and 254. The default value is **208**.

▶ **To use static information:**

1. Locate the *sntpUseDhcp* variable (under *sntpGroup*).

   This variable defines whether the AT-VP504E FXS must ask for its SNTP server settings through a DHCP server or not.

2. Set the *sntpUseDhcp* variable to **0=Static**.

3. Set the following variables:

Table 32: SNTP Static Address

Variable	Description
sntpStaticHost	Static SNTP server IP address or domain name. **Default Value**: 192.168.0.10
sntpStaticPort	Static SNTP server IP port number. **Default Value**: 123

Selecting a Time Zone

At boot time, the AT-VP504E FXS communication unit queries a NTP server to receive time information. The unit receives the information in Universal Time Coordinated (UTC) format (also known as GMT time), so it needs to convert this UTC time into the proper time zone. To do this, the AT-VP504E FXS offers time zone configuration with daylight saving settings.

▶ **To set time zone information:**

1. Set the *sntpTimeZoneUseTimeZoneSelection* variable (under *sntpTimeZoneConfigGroup*).

   This variable defines whether the AT-VP504E FXS must use pre-configured or customized time zones. Available values are:

   - 0 = Use custom time zone configuration
   - 1 = Use pre-configured time zone selection

   The default value is **1 = Use pre-configured time zone selection**.

2. If you are using pre-configured time zones, select the proper time zone in the *sntpTimeZoneTimeZoneSelection* variable (under *sntpTimeZoneConfigGroup*).

   The clock is automatically adjusted for daylight saving time changes, if applicable. Available values are:

   - 0 = Pacific Time (Canada & US) (GMT - 8h)
   - 1 = Mountain Time (Canada & US) (GMT - 7h)
   - 2 = Central Time (Canada & US) (GMT - 6h)
   - 3 = Eastern Time (Canada & US) (GMT - 5h)
   - 4 = Atlantic Time (Canada) (GMT - 4h)
   - 5 = GMT Standard Time

- 6 = W. Europe Standard Time (GMT + 1h)
- 7 = China Standard Time (GMT + 8h)
- 8 = Tokyo Standard Time (GMT + 9h)
- 9 = Central Australia Standard Time (GMT + 9h30)
- 10 = Australia Eastern Standard Time (GMT + 10h)

The default value is **1**. The pre-configured time zones available are:

Table 33: Pre-Configured Time Zones

Time zone	GMT Offset	Daylight saving time			POSIX String
		GMT Offset	Starting Date	Ending Date	
Pacific Time (Canada & US)	-08:00	-07:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	PST8DST7,M4.1.0/02:00:00,M10.5.0/ 02:00:00
Mountain Time (Canada & US)	-07:00	-06:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	MST7DST6,M4.1.0/02:00:00,M10.5.0/ 02:00:00
Central Time (Canada & US)	-06:00	-05:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	CST6DST5,M4.1.0/02:00:00,M10.5.0/ 02:00:00
Eastern Time (Canada & US)	-05:00	-04:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	EST5DST4,M4.1.0/02:00:00,M10.5.0/ 02:00:00
Atlantic Time (Canada)	-04:00	-03:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	AST4DST3,M4.1.0/02:00:00,M10.5.0/ 02:00:00
GMT Standard Time	-00:00	+01:00	Last Sunday of March at 01:00:00 AM	Last Sunday of October at 02:00:00 AM	GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/ 02:00:00
W. Europe Standard Time	+01:00	+02:00	Last Sunday of March at 02:00:00 AM	Last Sunday of October at 03:00:00 AM	WEST-1DWEST-2,M3.5.0/ 01:00:00,M10.5.0/03:00:00
China Standard Time	+08:00	None	N/A	N/A	CST-8
Tokyo Standard Time	+09:00	None	N/A	N/A	TST-9
Central Australia Standard Time	+09:30	+10:30	Last Sunday of October at 02:00:00 AM	Last Sunday of March at 02:00:00 AM	CAUST-9:30DCAUST-10:30,M10.5.0/ 02:00:00,M3.5.0/02:00:00
Australia Eastern Standard Time	+10:00	+11:00	Last Sunday of October at 02:00:00 AM	Last Sunday of March at 02:00:00 AM	AUSEST-10AUSDST-11,M10.5.0/ 02:00:00,M3.5.0/02:00:00

3. If you are using customized time zones, set the custom time zone POSIX string in the *sntpTimeZoneCustomTimeZone Configuration* variable (under *sntpTimeZoneConfigGroup*).

   The default POSIX string is:

   `EST5DST4,M4.1.0/02:00:00,M10.5.0/02:00:00`

Defining a Custom Time Zone

To define a custom time zone, you must enter a valid POSIX (Portable Operating System Interface) string. A POSIX string is a set of standard operating system interfaces based on the UNIX operating system. This standard is used in the time zone string in the format:

`STD[OFFSET]DLST[OFFSET],[START[/TIME]],[END[/TIME]]`

Table 34: Custom Time Zone Settings

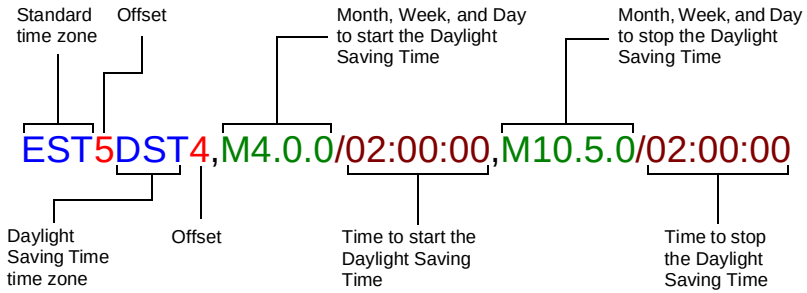
Setting	Definition
STD and DLST	Three or more characters for the standard (STD) or alternative daylight saving time (DLST) time zone. Only STD is mandatory. If DLST is not supplied, the daylight saving time does not apply. Lower and upper case letters are allowed. All characters are allowed except digits, leading colon (:), comma (,), minus (-), plus (+), and ASCII NUL.
OFFSET	Difference between the local time and the GMT time. The offset has the format *h[h][:m[m][:s[s]]]*. If no offset is supplied for DLST, the alternative time is assumed to be one hour ahead of standard time. One or more digits can be used; the value is always interpreted as a decimal number. The hour value must be between 0 and 24. The minute and seconds values, if present, must be between 0 and 59. If preceded by a minus (-), the time zone is east of the prime meridian, otherwise it is west, which can be indicated by the preceding plus sign (+). For example, New York time is GMT+5.

Table 34: Custom Time Zone Settings (Continued)

Setting	Definition
START and END	Indicates when to change to and return from the daylight saving time. The *START* argument is the date when the change from the standard to the daylight save time occurs; *END* is the date for changing back. If *START* and *END* are not specified, the default is the US Daylight saving time start and end dates. The format for start and end must be **one** of the following: • **n** where *n* is the number of days since the start of the year from 1 to 365. It must contain the leap year day if the current year is a leap year. With this format, it is your responsibility to determine all the leap year details. • **Jn** where *n* is the number of days since the start of the year from 1 to 365. Leap days are not counted. The *TIME* parameter has the same format as *OFFSET* but there can be no leading minus (-) or plus (+) sign. If *TIME* is not specified, the default is *02:00:00*. • **Mx[x].y.z** where *x* is the month, *y* is a week count and *z* is the day of the week starting at 0 (Sunday). As an example, *M10.5.0* is the Sunday of the fifth week of October. The *TIME* parameter has the same format as *OFFSET* but there can be no leading minus (-) or plus (+) sign. If TIME is not specified, the default is *02:00:00*.

Example

The following is an example of a proper POSIX string:


Standard time zone
Offset
Month, Week, and Day to start the Daylight Saving Time
Month, Week, and Day to stop the Daylight Saving Time
EST5DST4,M4.0.0/02:00:00,M10.5.0/02:00:00
Daylight Saving Time time zone
Offset
Time to start the Daylight Saving Time
Time to stop the Daylight Saving Time

10 Maintenance

This chapter explains how to maintain the AT-VP504E FXS. It also contains a troubleshoothing section that helps you find and correct the most common problems you may encounter with the AT-VP504E FXS.

Warning

To prevent fire or shock hazard do not expose this unit to rain or moisture.

Caution Regarding Handling

The AT-VP504E FXS is in fact a small computer device that must be handled with some caution. This section illustrates the basic facts regarding handling, storage and cleaning.

Location

Install the AT-VP504E FXS in a well ventilated location where it will not be exposed to high temperature or humidity.

Do not install the AT-VP504E FXS in a location exposed to direct sunlight or near stoves or radiators. Excessive heat could damage the internal components.

Condensation

When the unit is brought into a warm environment from the cold, condensation may result which might be harmful to the unit. If this occurs, allow the unit to acclimatize for an hour before powering it on.

Cleaning

To clean the AT-VP504E FXS, wipe with a soft dry cloth. Do not use volatile liquids such as benzine and thinner which are harmful to the unit casing.

For resistant markings, wet a cloth with a mild detergent, wring well then wipe off. Use a dry cloth to dry the surface.

Troubleshooting

The AT-VP504E FXS is very simple to install and operate, but you could experience some minor problems when it is connected to the network. The following section will examine some of these problems and possible solutions.

Note: Problems encountered by the AT-VP504E FXS are listed in a Syslog message. You can see this message with the Syslog daemon.

Solving General Operation Problems

Unit does not operate – All LEDs are OFF

Power is not fed to the unit. Check that:

- The power cable is connected to the AC socket.
- The power cable is fully inserted into the AT-VP504E FXS power socket.

Impossible to make a call

If the following happens:

- Dial tone present.
- Power LED lit.
- LAN LED lit.

Network communication is not working. Check that:

- The LAN cable network is securely connected to the AT-VP504E FXS and to the network connector.
- You did not connect a cross-over network cable.

Impossible to make a call to a destination

If the following happens:

- Dial tone present.
- Power LED lit.
- Test LED lights up when the phone goes off hook.
- LAN LED lit.

Configurable parameters of the AT-VP504E FXS are not set properly.

- Refer to this manual for a complete description of the configurable AT-VP504E FXS parameters.

"Poor line condition" error during a fax transmission

The analog transmission between the fax machine and the AT-VP504E FXS is flaky, preventing the fax transmission to terminate properly. This problem is known to occur with some fax machines and it can also occur with a few fax modems. To remedy the problem:

- Set the *Input sound level* to **-6dB**. If this still does not solve the problem, try the **+6dB** value. See "Setting User Gain Variables" on page 57 for more details.

Solving Software Upgrade Problems

An error occurs when the AT-VP504E FXS attempts to communicate with the software server

There could be a number of reasons for this:

- The file specified in the upgrade command does not exist or is in a different directory to the one given.
  - Check the file name and its location.
  - Make sure that the software server (TFTP) is running and properly configured.
- The IP address of the software server is not the correct one.
  - Check the given IP address.
  - Check the IP port.

An error occurs when the AT-VP504E FXS attempts to transfer the file

There could be a number of reasons for this:

- The Ethernet cable has become disconnected from the AT-VP504E FXS or the PC running the file transfer. Reconnect the cable and start again.
- Power to the AT-VP504E FXS has been disrupted during the file transfer. Check the power connection to the AT-VP504E FXS and start again.
- An incorrect file is being specified and transferred to the AT-VP504E FXS. Check the filename and start again.

Solving SNMP Management Software Problems

The SNMP network management software cannot access the AT-VP504E FXS

Check that:

- The IP information for the AT-VP504E FXS is correctly configured.
- The AT-VP504E FXS was reset after the IP information was defined.

Try to locate the AT-VP504E FXS's IP address. If impossible, perform a reset as indicated in section "Using the Dual-Mode Default Settings Switch" on page 22.

Traps are not received by the SNMP network manager

Check that:

- The IP information (IP address + IP port) of the SNMP Network manager software is correctly recorded by the AT-VP504E FXS.

The SNMP Network Management software can no longer access the AT-VP504E FXS

Check that:

- The port through which you are trying to access the AT-VP504E FXS has been disabled or is not the correct port. If it is enabled, check the connections and network cabling for the port.

Part 2:
SIP-Specific Settings

Signalling Protocol Configuration – SIP

The AT-VP504E FXS uses SIP signalling programs and information defined in a SIP stack to work properly. This includes SIP Log information, server addresses, etc.

Setting up the SIP Logging Client

The SIP Logging Client information is used to log the incoming and outgoing SIP packets.

▶ **To enable SIP Logs:**

1. In the SIP MIB, locate the *sipUALogEnable* variable (under *sipUALogGroup*).

   This variable allows the stack to log SIP packets.

2. Set the *sipUALogEnable* variable to **1=Enable**.

3. Set the IP port number for SIP User Agents in the *sipUAPort* variable (under *sipUAGroup*).

   The default port value is **5060**.

DHCP vs. Static Configuration

The SIP User Agents information can be assigned through a DHCP server or set statically.

▶ **To use DHCP-assigned information:**

1. In the SIP MIB, locate the *sipUALogUseDhcp* variable (under *sipUALogGroup*).

   This variable defines whether the AT-VP504E FXS must ask for its SIP Log settings through a DHCP server or not.

2. Set the *sipUALogUseDhcp* variable to **1=DHCP**.

   You can query the SIP Logging Client's IP address and Port number assigned by the DHCP server in the *sipUALogDhcp Host* and *sipUALogDhcpPort* read-only variables.

3. Set the DHCP Vendor Specific code of the SIP Logging Client in the *sipUALogDhcpVendorSpecificCode* variable.

   This code can be any number between 0 and 254. The default value is **202**.

▶ **To use static information:**

1. In the SIP MIB, locate the *sipUALogUseDhcp* variable (under *sipUALogGroup*).

   This variable defines whether the AT-VP504E FXS must ask for its SIP Log settings through a DHCP server or not.

2. Set the *sipUALogUseDhcp* variable to **0=Static**.

3. Set the following variables:

Table 35: SIP Logging Client Static Address

Variable	Description
sipUALogStaticHost	SIP Logging Client static IP address or domain name. **Default Value**: 192.168.0.10
sipUALogStaticPort	SIP Logging Client static IP port number. **Default Value**: 6000

Setting up SIP User Agents Servers

The SIP stack uses two types of servers that have their specific tasks: the Registrar server and Proxy server.

DHCP vs. Static Configuration

The SIP servers information can be assigned through a DHCP server or set statically.

▶ **To use DHCP-assigned information:**

1. In the SIP MIB, locate the *sipUAServerUseDhcp* variable (under *sipUAServerGroup*).

   This variable defines whether the AT-VP504E FXS must get its SIP Server configuration through a DHCP Server or not.

2. Set the *sipUAServerUseDhcp* variable to **1=DHCP**.

   You can query the SIP Server's IP address and port number assigned by the DHCP server in the following read-only variables:

   - sipUAServerDhcpRegistrarHost
   - sipUAServerDhcpRegistrarPort

- sipUAServerDhcpProxyHost
- sipUAServerDhcpProxyPort

3. Set the DHCP Vendor Specific code of the SIP Registrar Server in the *sipUAServerDhcpRegistrarVendorSpecific Code* variable.

   This code can be any number between 0 and 254. The default value is **203**.

4. Set the DHCP Vendor Specific code of the SIP Proxy Server in the *sipUAServerDhcpProxyVendorSpecificCode* variable.

   This code can be any number between 0 and 254. The default value is **204**.

▶ **To use static information:**

1. In the SIP MIB, locate the *sipUAServerUseDhcp* variable (under *sipUAServerGroup*).

   This variable defines whether the AT-VP504E FXS must get its SIP Server configuration through a DHCP Server or not.

2. Set the *sipUAServerUseDhcp* variable to **0=Static**.

3. Set the following variables:

Table 36: SIP Server Static Address

Variable	Description
sipUAServerStaticRegistrar Host	SIP Registrar server static IP address or domain name. **Default Value**: 192.168.0.10
sipUAServerStaticRegistrarPort	SIP Registrar server static IP port number. **Default Value**: 5060
sipUAServerStaticProxyHost	SIP Proxy server static IP address or domain name. **Default Value**: 192.168.0.10
sipUAServerStaticProxyPort	SIP Proxy server static IP port number. **Default Value**: 5060

Defining SIP User Agents

The AT-VP504E FXS has four FXS lines. Each line is defined as a SIP User Agent. You can set information for each SIP User Agent such as its telephone number and friendly name. The telephone number and friendly name (an identification name) make up the Caller ID information that is displayed on telephones/faxes equipped with a proper LCD display.

▶ To set User Agent information:

1. In the SIP MIB, locate the *sipUA1Group* category.
2. Set the following information:

Table 37: SIP User Agent Information

Variable	Description
sipUA1PrefixCCAndAC	Select if the Country Code and Area Code must be prefixed to the main alias for SIP User Agent #1. • 0 = Do not prefix Country Code and Area Code • 1 = Prefix Country Code and Area Code **Default Value**: 1
sipUA1MainAlias	Main alias (telephone number) for SIP User Agent #1. **Default Value**: 3331111
sipUA1FriendlyName	Friendly name for SIP User Agent #1. **Default Value**: Port 1
sipUA1OtherAliases	Semi-colon separated list of other aliases for SIP User Agent #1. An alias is either a user name or a telephone number.
sipUA1MustUse SessionTimers	Select if the session timer must be used. • 0 = Don't use session timer. • 1 = Must use session timer. **Default Value**: 0

Table 37: SIP User Agent Information (Continued)

Variable	Description
sipUA1Maximum SessionExpirationDelay	Set the maximun session expiration delay in seconds. If *sipUA1MustUseSessionTimers* is set to 1, then an INVITE is sent every *n* seconds, where *n* is specified in the *sipUA1MaximumSessionExpirationDelay* variable. If an INVITE does not get an answer, then the call is terminated. This option allows to detect the end of a call caused by a communication problem on the network. If *sipUA1MustUseSessionTimers* is set to 0 and the network is cut off between the two telephones, then it will not be possible to detect the end of the call, because no end of communication packet will be received. **Default Value**: 60

Note: You can repeat the same process for each port of the AT-VP504E FXS.

Authentication Information

Authentication information allows you to add some level of security to the AT-VP504E FXS lines by setting user names and passwords.

Username and Password Syntax

The syntax of the authentication variables is as follows:

```
"realm1"="username1":"password1";"realm2"="username2":"password2";.."realmn"="usernamen":"passwordn";
```

Note that `realm`, `username` and `password` are enclosed in quotation marks. For example:

```
"ABC Inc" = "John Smith":"Hello"
```

Notes:

- If the syntax of *AuthUsrPwd* is valid, its corresponding read-only *AuthValid* is set to 1; if not, it is set to 0.
- The same realm cannot appear twice in the same variable, or one of them will be ignored.
- If a realm is in the general variable and in a port-specific variable, the port-specific password and username will be used.

- Spaces outside the quotation marks are ignored.
- If you want to use the quotation mark character in a string, you must precede it with \.

  Example:

  ```
  "ABC Inc" = "John \"Jake\" Smith":"Hello"
  ```

Adding a User Name and Password

To add a user name and password that apply to all ports:

1. In the SIP MIB, locate the *sipUAAuthUsrPwd* variable in the *sipUAAuthGroup*.

   This variable is used to define the username and password used for authentication. This value is used by all ports.

2. Set a username and password for this variable according to the following syntax:

   ```
   "realm1"="username1":"password1";"realm2"="username2":"password2";.."realmn"="usernamen":"passwordn";
   ```

   Refer to "Username and Password Syntax" on page 89 for details on how to define this variable.

To add individual user names and passwords for each port:

1. In the SIP MIB, locate the *sipUA1AuthUsrPwd* variable in the *sipUA1AuthGroup*.

   This is the username and password used for authentication. This value is used only by this port.

2. Set a username and password for this variable according to the following syntax:

   ```
   "realm1"="username1":"password1";"realm2"="username2":"password2";.."realmn"="usernamen":"passwordn";
   ```

   Refer to "Username and Password Syntax" on page 89 for details on how to define this variable.

Note: You can repeat the same process for each port of the AT-VP504E FXS.

12 Telephony Configuration

This chapter explains how to set the telephony variables of the AT-VP504E FXS, i.e. the way the unit handles calls.

Using Dial Maps

A Dial Map is a very powerful feature that allows you to compare the number users just dialed to a string of arguments. If they match, users will be able to make the call. If not, users will not be able to make the call and will get a busy signal. It is thus essential to define very precisely a Dial Map before actually implementing it, or your users may encounter calling problems.

Because the AT-VP504E FXS cannot predict how many digits it needs to accumulate before transmission, you could use the Dial Map, for instance, to determine exactly when there are sufficient digits entered from the user to place a call.

For example, using the phone on your desk, you can dial the following numbers:

Table 38: Number Examples

Number	Description
0	Local operator
00	Long distance operator
xxxx	Local extension number
8xxxxxxx	Local number
#xxxxxxx	Shortcut to local number at other corporate sites
91xxxxxxxxxx	Long distance numbers
9011 + up to 15 digits	International number

The solution to this problem is to load the AT-VP504E FXS with a Dial Map that corresponds to the dial plan. This Dial Map is expressed using a specific syntax.

An AT-VP504E FXS that detects digits or timers applies the current dial string to the Dial Map, attempting a match to each regular expression in the Dial Map in lexical order.

- If the result is under-qualified (partially matches at least one entry in the Dial Map), waits for more digits.
- If the result matches, dials the number.

- If the result is over-qualified (i.e. no further digits could possibly produce a match), sends a fast busy signal.

Using the Dial Map Special Characters

Dial Maps use specific characters and digits in a particular syntax. Those characters are:

Table 39: Dial Map Characters

Character	Use
Digits (0, 1, 2... 9)	Indicates specific digits in a telephone number expression.
T	The Timer indicates that if users have not dialed a digit for 4 seconds, it is likely that they have finished dialing and the IP Communication Server can make the call.
x	Matches any digit, including “#” and “*”.
|	Indicates a choice of matching expressions (OR).
.	Matches an arbitrary number of occurrences of the preceding digit, including 0.
[	Indicates the start of a range of characters.
]	Indicates the end of a range of characters.

How to Use a Dial Map

Let’s say you are in an office and you want to call a co-worker’s 3-digit extension. You could build a Dial Map that said “after the user has entered 3 digits, make the call”. The Dial Map could look as follows:

```
xxx
```

This Dial Map specifies that after the user has entered any three digits, the call is placed. You could refine this Dial Map by including a range of digits. For example, you know that all extensions in your company either begin with 2, 3, or 4. The corresponding Dial Map could look as follows:

```
[2-4]xx
```

You have just entered a range of digit. Thus, if the number you dial begins by anything other than 2, 3, or 4, the call will not be placed and you will get a busy signal. Another way to achieve the same result would be:

```
[234]xx
```

Combining Several Expressions in a Dial Map

It is possible to combine two or more expressions in the same Dial Map by using the "|" operator, which is equivalent to OR.

Let's say you want to specify a choice: the Dial Map is to check if the number is internal (extension), or external (a local call). Assuming that you must first dial "9" to make an external call, you could define a Dial Map as follows:

```
[2-4]xx|9[2-9]xxxxxx
```

The Dial Map checks if:

- the number begins by 2, 3, or 4 **and**
- the number has 3 digits

If not, it checks if:

- the number begins with 9 **and**
- the second digit is any digit between 2 and 9 **and**
- the number has 7 digits

Using the # and * Characters

It may sometimes be required that users dial the "#" or "*" to make calls. This can be easily incorporated in a Dial Map:

```
xxxxxxx#
xxxxxxx*
```

The "#" or "*" character could indicate users must dial the "#" or "*" character at the end of their number to indicate it is complete.

Note: When making the actual call and dialing the number, the AT-VP504E FXS automatically removes the "#" or "*" found at the end of a dialed number, if there is one (after a match). Those characters are for indication purposes only.

Using the Timer

The Timer is set at 4 seconds. It indicates that if users have not dialed a digit for 4 seconds, it is likely that they have finished dialing and the gateway can make the call. A Dial Map for this could be:

```
[2-9]xxxxxxT
```

Note: When making the actual call and dialing the number, the AT-VP504E FXS automatically removes the “T” found at the end of a dialed number, if there is one (after a match). This character is for indication purposes only.

Using a Dial Map for Calls Outside the Country

If your users are making calls outside your country, it may sometimes be hard to determine exactly the number of digits they will have to enter. You could devise a Dial Map that takes this problem into account:

```
001x.T
```

Where the Dial Map looks for a number that begins with 001, then any number of digits after that (x.).

Example

Table 38 on page 91 outlined various call types one could make. All these possibilities could be covered in one Dial Map:

0T|00T|[1-7]xxx|8xxxxxxx|#xxxxxxx|91xxxxxxxxxx|9011x.T

Validating a Dial Map

If you enter a Dial Map expression in one of the Dial Map rules, the AT-VP504E FXS will validate the Dial Map and indicate if it is correct or not.

Setting up Dial Maps

The Provisioning MIB allows to create four (4) different Dial Map rules. These rules are located under the group *apaUIMapRuleGroup* and labelled as follows:

- apaUIMapRule1Group
- apaUIMapRule2Group
- apaUIMapRule3Group
- apaUIMapRule4Group

Dial Maps follow these rules:

- Dial Map rules are checked sequentially. If a phone number potentially matches two of the rules, the first rule encountered will be applied.
- Dial Map rules assume that you have properly set the *Area Code* and *Country Code* variables in the

countryGroup section of the Provisioning MIB.

Each of these Dial Map rules has seven (7) specific variables that you must define for the Dial Map to work properly. For example, the following are the variables associated with Dial Map #1.

Table 40: Dial Map Rules Variables

Variable	Description
apaUIMapRule1 Enable	**Possible Values**: • 0 = Disable • 1 = Enable When selecting **1**, the AT-VP504E FXS will compare the number users dial to the valid Dial Map for a match. Keep in mind that you can have up to four (4) Dial Map Rules active. Each of them will be compared and, if there is a match with any of the rules, the call will be made.
apaUIMapRule1 DialMap	Actual Dial Map string to which the number will be compared. This Dial Map will be validated. A valid Dial Map could be: 011x.T|011x.#|1xxxxxxxxxx|[2-8]xxxxxx
apaUIMapRule1 IsValid	**Possible Values**: • 0 = Not valid • 1 = Valid The AT-VP504E FXS will validate the Dial Map after a SNMP set. The result (valid, invalid) is displayed.
apaUIMapRule1 RemDigitEnable	Indicates if digits are to be removed from the number dialed by users when making the call. A complete and valid telephone number must contain a Country Code, an Area Code, and a number. **Possible Values**: • 0 = Disable • 1 = Enable
apaUIMapRule1 RemDigitCount	If the *apaUIMapRule1RemDigitEnable* variable is enabled, specifies the number of digits to remove from the number dialed by users. Digits are removed at the beginning of the dial string.

Table 40: Dial Map Rules Variables (Continued)

Variable	Description
apaUIMapRule1 PrefixEnable	Indicates if digits are to be added to the number dialed by users when making the call. A complete and valid telephone number must contain a Country Code, an Area Code, and a number. **Possible Values**: • 0 = Disable • 1 = Enable
apaUIMapRule1 PrefixDigit	If the *apaUIMapRule1PrefixEnable* variable is enabled, adds the selected digits to the number dialed by users. **Possible Values**: • 0 - Prefix Area code • 1 - Prefix Country code • 2 - Prefix Country code and Area code

Note: Similar variables apply to the other three dial map rules.

Dial Map Examples

The following examples will help you set up various scenarios that could apply to your situation. You can use up to four (4) Dial Map rules. Each time a user dials a digit, the number is compared to the rules and, if there is a match, the number is dialed.

Example 1 – Standard Calls

Let's say you are located in Seattle, Washington and you want to define Dial Map rules for your users. You must consider at least four possibilities:

- You are making a long distance call outside the country.
- You are making a long distance call outside your Area Code.
- You are making a local call outside your Area Code (in the 425 Area Code).
- You are making a local call in the same Area Code.

Dial Map Rule #1 – apaUIMapRule1Group

This Dial Map rule checks for calls outside the country.

Table 41: Dial Map Rules #1 Settings

Variable	Setting
apaUIMapRule1Enable	1 = Enable
apaUIMapRule1DialMap	011x.#|001x.T
apaUIMapRule1RemDigitEnable	1 = Enable
apaUIMapRule1RemDigitCount	3 A valid telephone number must contain a Country Code, an Area Code, and a number. The Country Code and Area Code are defined in the *countryGroup* section and the "011" part is thus not required.
apaUIMapRule1PrefixEnable	0 = Disable

Dial Map Rule #2

This Dial Map rule checks for long distance calls outside your Area Code.

Table 42: Dial Map Rules #2 Settings

Variable	Setting
apaUIMapRule2Enable	1 = Enable
apaUIMapRule2DialMap	1xxxxxxxxxx
apaUIMapRule2RemDigit Enable	1 = Enable

Table 42: Dial Map Rules #2 Settings (Continued)

Variable	Setting
apaUIMapRule2RemDigit Count	1 The first digit “1” in the dial map indicates a user wants to call outside his/her own Area Code. It has to be removed because it does not need to be expressed to the IP Communication Server. The IP Communication Server needs only to know the complete number of the called party (CC+AC+directory number).
apaUIMapRule2PrefixEnable	1 = Enable
apaUIMapRule2PrefixDigit	1 - Prefix Country code A valid telephone number must contain a Country Code, an Area Code, and a number. The Country Code is missing in this number and must be added. Note that in this scenario, the Country Code is the same code as the code used when the user wants to indicate a communication outside of his/her own Area Code. It is still good practice to have this number removed and to add the country code, event if these two numbers are the same.

Dial Map Rule #3

This Dial Map rule checks for local calls outside your Area Code (in the 425 Area Code).

Table 43: Dial Map Rules #3 Settings

Variable	Setting
apaUIMapRule3Enable	1 = Enable
apaUIMapRule3DialMap	425xxxxxxx
apaUIMapRule3RemDigit Enable	0 = Disable
apaUIMapRule3PrefixEnable	1 = Enable

Table 43: Dial Map Rules #3 Settings (Continued)

Variable	Setting
apaUIMapRule3PrefixDigit	1 - Prefix Country code A valid telephone number must contain a Country Code, an Area Code, and a number. The Country Code is missing in this number and must be added.

Dial Map Rule #4

This Dial Map rule checks for local calls in the same Area Code.

Table 44: Dial Map Rules #4 Settings

Variable	Setting
apaUIMapRule4Enable	1 = Enable
apaUIMapRule4DialMap	[235-9]xxxxxx|45[1-9]xxxx|4[0-469]xxxxx
apaUIMapRule4RemDigit Enable	0 = Disable
apaUIMapRule4Prefix Enable	1 = Enable
apaUIMapRule4PrefixDigit	2 - Prefix Country code and Area code A valid telephone number must contain a Country Code, an Area Code, and a number. The Country Code and Area Code are missing in this number and must be added.

You could further refine these Dial Maps according to your needs. Experiment with Dial Maps.

Example 2 – PBX Emulation

Let's say you are located in the 819 Area Code. You are in an office where you must dial:

- 3 numbers to call one of your co-workers.
- 9 to get an external line.

The following four possibilities are considered:

- You are making an internal call to one of your co-workers.

- You are making a long distance call outside the country.
- You are making a long distance call outside your Area Code.
- You are making a local call in the same Area Code.

Dial Map Rule #1

This Dial Map rule checks for internal calls.

Table 45: Dial Map Rules #1 Settings

Variable	Setting
apaUIMapRule1Enable	1 = Enable
apaUIMapRule1DialMap	[1-8]xx
apaUIMapRule1RemDigit Enable	0 = Disable
apaUIMapRule1PrefixEnable	1 = Enable
apaUIMapRule1PrefixDigit	2 - Prefix Country code and Area code A valid telephone number must contain a Country Code, an Area Code, and a number. The Country Code and Area Code are missing in this number and must be added.

Dial Map Rule #2

This Dial Map rule checks for calls outside the country.

Table 46: Dial Map Rules #2 Settings

Variable	Setting
apaUIMapRule2Enable	1 = Enable
apaUIMapRule2DialMap	9011x.#|9011x.T
apaUIMapRule2RemDigit Enable	1 = Enable

Table 46: Dial Map Rules #2 Settings (Continued)

Variable	Setting
apaUIMapRule2RemDigit Count	4 A valid telephone number must contain a Country Code, an Area Code, and a number. The Country Code and Area Code are defined in the *countryGroup* section and the “9011” part is thus not required.
apaUIMapRule2PrefixEnable	0 = Disable There is no need to prefix any more digit to the dialed number because this type of international call already specifies the Country Code and Area Code.

Dial Map Rule #3

This Dial Map rule checks for long distance calls outside your Area Code.

Table 47: Dial Map Rules #3 Settings

Variable	Setting
apaUIMapRule3Enable	1 = Enable
apaUIMapRule3DialMap	91xxxxxxxxx
apaUIMapRule3RemDigit Enable	1 = Enable
apaUIMapRule3RemDigit Count	2 The first digit “9” in the dial map indicates a user wants to make an external call, while the second digit “1” indicates a user wants to call outside his/her own Area Code (in North America). The two digits must be removed because they do not need to be expressed to the IP Communication Server. The IP Communication Server needs only to know the complete number of the called party (CC+AC+directory number).

Table 47: Dial Map Rules #3 Settings (Continued)

Variable	Setting
apaUIMapRule3PrefixEnable	1 = Enable
apaUIMapRule3PrefixDigit	1 - Prefix Country code A valid telephone number must contain a Country Code, an Area Code, and a number. The Country Code is missing in this number and must be added. Note that in this scenario, the Country Code is the same code as the code used when the user wants to indicate a communication outside of his/her own Area Code. It is still good practice to have this number removed and to add the country code, event if these two numbers are the same.

Dial Map Rule #4

This Dial Map rule checks for local calls in the same Area Code.

Table 48: Dial Map Rules #2 Settings

Variable	Setting
apaUIMapRule4Enable	1 = Enable
apaUIMapRule4DialMap	9[2-8]xxxxxx
apaUIMapRule4RemDigit Enable	1 = Enable
apaUIMapRule4RemDigit Count	1 The first digit “9” in the dial map indicates a user wants to make an external call. It has to be removed because it does not need to be expressed to the IP Communication Server. The IP Communication Server needs only to know the complete number of the called party (CC+AC+directory number).
apaUIMapRule4PrefixEnable	1 = Enable

Table 48: Dial Map Rules #2 Settings (Continued)

Variable	Setting
apaUIMapRule4PrefixDigit	2 - Prefix Country code and Area code A valid telephone number must contain a Country Code, an Area Code, and a number. The Country Code and Area Code are missing in this number and must be added.

You could further refine these Dial Maps according to your needs. Experiment with Dial Maps.

Supplementary Telephony Services

The AT-VP504E FXS offers telephony services one can use directly on his/her phone. However, you must set these services before they can be used.

Call Forward

The Call Forward feature offers various ways to forward calls:

- Unconditional
- On Busy
- On No Answer

Unconditional

The Call Forward – Unconditional feature allows users to forward their calls to another extension or line.

To set the Call Forward Unconditional feature:

1. Locate the *apaUIServicesPort1CallForwardUnconditional Group* category of the Provisioning MIB.

   This group contains all of the variables required to set the Call Forward Unconditional feature.

2. Enable the Call Forward Unconditional by setting the *apaUIServicesPort1CallForwardUnconditionalEnable* variable to **1**.

3. Define the SIP URL to which incoming calls will be forwarded in the *apaUIServicesPort1CallForwardUnconditionalAddress* variable.

   A SIP URL has the following format:

   `userInfo@host:portNumber`

   The `userInfo` part is either a user name or a telephone number. The `host` part is either a domain name or an IP address. A valid SIP URL could be:

   `18198298749@192.168.0.1:5060`

4. Define the digits that users will have to dial to start the Call Forward Unconditional feature in the *apaUIServicesPort1 CallForwardUnconditionalEnableStarNumber* variable.

   Users must dial the "*xx" sequence to start the feature on their telephone, where "xx" is the value attributed in the current variable. The "xx" value must be between 10 and 99 and different from the value set in Step 5.

5. Define the digits that users will have to dial to stop the Call Forward Unconditional feature in the *apaUIServicesPort1 CallForwardUnconditionalDisableStarNumber* variable.

   Users must dial the "*xx" sequence to disable the feature on their telephone, where "xx" is the value attributed in the current variable. The "xx" value must be between 10 and 99 and different from the value set in Step 4.

Note: You can repeat the same process for each port of the AT-VP504E FXS.

On Busy

You can automatically forward the incoming calls of your users to a pre-determined extension within your system if they are already on the line.

Note: The call forward on busy can only be set up by you. Users cannot enable it from their telephone.

▶ **To set the Call Forward On Busy feature:**

1. Locate the *apaUIServicesPort1CallForwardBusyGroup* category of the Provisioning MIB.

   This group contains all of the variables required to set the Call Forward On Busy feature.

2. Enable the Call Forward On Busy by setting the *apaUIServicesPort1CallForwardBusyEnable* variable to **1**.

3. Define the SIP URL to which incoming calls will be automatically forwarded in the *apaUIServicesPort1Call ForwardBusyAddress* variable.

   A SIP URL has the following format:

   `userInfo@host:portNumber`

   The `userInfo` part is either a user name or a telephone number. The `host` part is either a domain name or an IP address. A valid SIP URL could be:

   `18198298749@192.168.0.1:5060`

Note: You can repeat the same process for each port of the AT-VP504E FXS.

On No Answer

You can forward the incoming calls of your users to a pre-determined extension within your system if they do not answer their phone.

Note: The call forward on no answer can only be set up by you. Users cannot enable it from their telephone.

▶ **To set the Call Forward On No Answer feature:**

1. Locate the "*apaUIServicesPort1CallForwardNoAnswer Group*" category of the Provisioning MIB.

   This group contains all of the variables required to set the Call Forward On No Answer feature.

2. Enable the Call Forward On No Answer by setting the *apaUIServicesPort1CallForwardNoAnswerEnable* variable to **1**.

3. Define the SIP URL to which incoming calls will be forwarded in the *apaUIServicesPort1CallForwardNoAnswerAddress* variable.

   A SIP URL has the following format:

   `userInfo@host:portNumber`

   The `userInfo` part is either a user name or a telephone number. The `host` part is either a domain name or an IP address. A valid SIP URL could be:

   `18198298749@192.168.0.1:5060`

4. Define the number of phone rings before forwarding the incoming call in the *apaUIServicesPort1CallForward NoAnswerNumberOfRingsdigits* variable.

   The default value is 3.

Note: You can repeat the same process for each port of the AT-VP504E FXS.

Call Waiting There are no specific settings for this service. Please refer to the *AT-VP504E FXS User's Manual* for more details on how to use it.

Call Transfer – Supervised There are no specific settings for this service. Please refer to the *AT-VP504E FXS User's Manual* for more details on how to use it.

Call Transfer – Unsupervised There are no specific settings for this service. Please refer to the *AT-VP504E FXS User's Manual* for more details on how to use it.

Caller ID on Call Waiting There are no specific settings for this service. Please refer to the *AT-VP504E FXS User's Manual* for more details on how to use it.

Three-Way Conference Call There are no specific settings for this service. However, Allied Telesyn recommends to set the packetization time to 30 ms for better results. See "Selecting the Preferred Codec" on page 59 for more details.

Please refer to the *AT-VP504E FXS User's Manual* for more details on how to use the three-way conferencing feature.

Part 3:
MGCP-Specific Settings

13 Signalling Protocol Configuration – MGCP

This chapter describes how to set information exclusive to the MGCP signalling protocol. This chapter assumes that the AT-VP504E FXS communication unit currently runs the MGCP protocol or that you will switch the unit to this protocol. The MGCP signalling programs and information are defined in a MGCP stack. This includes Call Agent information and addresses, media package settings, etc.

Introduction

When the AT-VP504E FXS communication unit runs the MGCP protocol, it uses the *MGCP MIB*. This MIB is located in the Allied Telesyn MIB architecture. See "MIB Structure" on page 8 for more details.

Your unit must run the MGCP protocol or you must switch to this protocol.

▶ To use the MGCP MIB

1. In the Provisioning MIB, locate the *signalingProtocolsSwitch* variable under the *signalingProtocolsGroup*.

   This variable allows you to switch from one protocol to another.

2. Set the *signalingProtocolsSwitch* variable to **0=MGCP**.

   The default value is **1=SIP**. The AT-VP504E FXS communication unit reboots automatically. After the unit restarts, it will use the MGCP MIB. You will be able to set the parameters specific to this signalling protocol.

MGCP Information

The AT-VP504E FXS uses MGCP version draft-huitema-megaco-mgcp-v0r1-05. MGCP is a protocol for controlling Voice over IP (VoIP) Gateways from intelligent external call control elements. MGCP uses the Master/Slave concept, where external call control elements are the Masters, while the devices connected to them (such as the AT-VP504E FXS), are the Slaves and only obey orders given by the Master.

The AT-VP504E FXS is used with any MGCP Call Agent (also known as Connection Manager), which manages calls from and to the AT-VP504E FXS.

Services Provided

While the AT-VP504E FXS uses the MGCP protocol, it uses the services provided by the Call Agent. See your Call Agent documentation for more information.

Setting up Call Agents Information

The Call Agent is the server that sends the proper information to the AT-VP504E FXS unit and manages calls from and to the unit.

DHCP vs. Static Configuration

The Call Agent information can be assigned through a DHCP server or set statically. The AT-VP504E FXS can use two Call Agents: the primary and secondary.

▶ **To use DHCP-assigned information:**

1. In the MGCP MIB, locate the *mgcpConfigurationCallAgent UseDhcp* variable (under *mgcpConfigurationCallAgent Group*).

   This variable defines whether the AT-VP504E FXS must ask for its Call Agent settings through a DHCP server or not.

2. Set the *mgcpConfigurationCallAgentUseDhcp* variable to **1=DHCP**.

   You can query the Call Agent's IP address and Port number assigned by the DHCP server in the following variables:

   - mgcpConfigurationCallAgentDhcpPrimaryAddress
   - mgcpConfigurationCallAgentDhcpPrimaryPort Number
   - mgcpConfigurationCallAgentDhcpSecondaryAddress
   - mgcpConfigurationCallAgentDhcpSecondaryPort Number

3. Set the DHCP Vendor Specific code of the Call Agents in the *mgcpConfigurationCallAgentDhcpPrimaryVendorSpecificCode* and *mgcpConfigurationCallAgentDhcpSecondaryVendorSpecificCode* variables.

   These codes can be any number between 0 and 254. The default value for the Primary Call Agent is **206**, while the default value for the Secondary Call Agent is **207**.

▶ **To use static information:**

1. In the MGCP MIB, locate the *mgcpConfigurationCallAgent UseDhcp* variable (under *mgcpConfigurationCallAgent Group*).

   This variable defines whether the AT-VP504E FXS must ask for its Call Agent settings through a DHCP server or not.

2. Set the *mgcpConfigurationCallAgentUseDhcp* variable to **0=Static**.

3. Set the following variables:

Table 49: MGCP Call Agent Static Address

Variable	Description
mgcpConfigurationCallAgent StaticPrimaryAddress	Primary static Call Agent address. Can be a dotted IP string or a FQDN address. **Default Value**: 192.168.0.10
mgcpConfigurationCallAgent StaticPrimaryPortNumber	Primary static Call Agent UDP port number. **Default Value**: 2727
mgcpConfigurationCallAgent StaticSecondaryAddress	Secondary static Call Agent address. Can be a dotted IP string or a FQDN address. **Default Value**: 192.168.0.10
mgcpConfigurationCallAgent StaticSecondaryPortNumber	Secondary static Call Agent UDP port number. **Default Value**: 2727

Configuring End-points

Endpoints are originating or terminating devices such as phones or faxes.

▶ **To set endpoints information:**

1. In the MGCP MIB, locate the *mgcpConfigurationEpIdGroup* category.

   This group contains the endpoint information you must set.

2. Set the following variables:

Table 50: MGCP Endpoint Information

Variable	Description
mgcpConfigurationEpIdLocal NameTerm1	String that specifies the term of the endpoint name. **Default Value**: aaln
mgcpConfigurationEpId GatewayFqdnUseDns	Select the provenance of the Fully Qualified Domain Name (FQDN). • 0 = Static • 1 = DNS **Default Value**: 0
mgcpConfigurationEpIdStatic GatewayFqdn	Static Fully Qualified Domain Name (FQDN) of the unit.

Setting up Retransmission Parameters

Retransmission is a method of error control in which hosts receiving messages acknowledge the receipt of correct messages and do not acknowledge the receipt of incorrect messages. The lack of acknowledgement is an indication to the sending host that it should transmit the failed message again.

▶ **To set Retransmission information:**

1. In the MGCP MIB, locate the *mgcpConfiguration RetransmissionGroup* category.

   This group contains the retransmission information you must set.

2. Set the following variables:

Table 51: MGCP Retransmission Information

Variable	Description
mgcpConfiguration RetransmissionAlgorithm	Retransmission algorithm: • 0 = static • 1 = exponential • 2 = exponential with jitter **Default Value**: 2
mgcpConfiguration RetransmissionInitialPeriod	Retransmission initial period in ms. **Default Value**: 1000
mgcpConfiguration RetransmissionMaxPeriod	Retransmission maximum period in ms. • 0 = No maximum **Default Value**: 30000
mgcpConfiguration RetransmissionTimeout	Retransmission timeout in seconds. • -1 = infinite - always retransmit • 0 = none - never retransmit **Default Value**: 30
mgcpConfiguration RetransmissionRetryCount	Retransmission retry count. • -1 = infinite - always retransmit **Default Value**: 30
mgcpConfiguration RetransmissionRsipInitial Delay	Delay in ms since the last RSIP to wait before sending the first RSIP for a new endpoint that wants to register. This is to avoid restart avalanche. • 0 = Send immediately **Default Value**: 0

Configuring Packages

The MGCP MIB offers three packages:

- Generic Media Package
- DTMF Package
- Line Package

Generic Media Package

The Generic Media package groups the events and signals that can be observed on several types of endpoints, such as trunking gateways, access gateways or residential gateways.

To set Generic Media package information:

1. In the MGCP MIB, locate the *mgcpConfigurationGeneric MediaPackageGroup* category.

   This group contains the Generic Media package information you must set.

2. Set the following variables:

Table 52: MGCP Generic Media Package Information

Variable	Description
mgcpConfigurationGeneric MediaPackageRtDuration	Ring back tone timeout value in ms. **Default Value**: 180000
mgcpConfigurationGeneric MediaPackageRbkDuration	Ring back on connection tone timeout value in ms. **Default Value**: 180000

DTMF Package The DTMF package groups variables pertaining to the DTMFs.

▶ **To set DTMF package information:**

1. In the MGCP MIB, locate the *mgcpConfigurationDtmf PackageGroup* category.

   This group contains the DTMF information you must set.

2. Set the following variables:

Table 53: MGCP DTMF Package Information

Variable	Description
mgcpConfigurationDtmf PackageDefaultDigitMap	The default Digit Map to apply. **Default Value**: 0-9T
mgcpConfigurationDtmf PackageInterdigitTimerShort Duration	If the unit can't determine when the final digit has occurred, the timer value is set to a short duration. • -1 = infinite • 0 = none **Default Value**: 4000
mgcpConfigurationDtmf PackageInterdigitTimerLong Duration	If the unit can determine when the final digit has occurred, the timer value is set to a long duration. • -1 = infinite • 0 = none **Default Value**: 16000

Line Package The Line package groups variables that determine tone timeouts of the MGCP protocol Line Package.

▶ **To set Line package information:**

1. In the MGCP MIB, locate the *mgcpConfigurationLine PackageGroup* category.

   This group contains the information you must set.

2. Set the following variables:

Table 54: MGCP Line Package Information

Variable	Description
mgcpConfigurationLine PackageBzDuration	Busy tone timeout value in ms. **Default Value**: 30000
mgcpConfigurationLine PackageDlDuration	Dial tone timeout value in ms. **Default Value**: 16000
mgcpConfigurationLine PackageRgDuration	Ring tone timeout value in ms. **Default Value**: 180000
mgcpConfigurationLine PackageSlDuration	Stutter dial tone timeout value in ms. **Default Value**: 16000
mgcpConfigurationLine PackageOtDuration	Off hook warning tone timeout value in ms. **Default Value**: 65535000

Viewing Status Parameters

The MGCP MIB offers various read-only status information that can be queried. These variables are located under the *mgcpStatusGroup* category.

Table 55: MGCP Status Parameters

Variable	Description
mgcpStatusProtocolVersion	Version of the MGCP protocol.
mgcpStatusStackVersion	Version of the MGCP stack.
mgcpStatusCallAgentAddress	The address of the Call Agent to which the unit is currently registered. **Default Value**: 0.0.0.0
mgcpStatusCallAgentPort Number	Port number of the Call Agent. **Default Value**: 0

Table 55: MGCP Status Parameters

Variable	Description
mgcpStatusRegistered	Unit status • 0 = NOT REGISTERED - The unit has not been able to successfully register with the call agent. • 1 = REGISTERED - The unit is registered with the call agent whose IP address is in the *mgcpStatusCallAgent Address* variable. **Default Value**: 0
mgcpStatusEndpointId GatewayFqdn	Fully Qualified Domain Name (FQDN). **Default Value**: N/A

Viewing MGCP Statistics

The MGCP MIB offers various read-only statistics pertaining to the MGCP protocol. These statistics are located under the *mgcpStatistics Group* category.

Table 56: MGCP Status Parameters

Variable	Description
mgcpStatisticsNumberOf ActiveConnections	Number of active connections. **Default Value**: 0
mgcpStatisticsTotalNumberOf Connections	Total number of connections since the last start up. **Default Value**: 0
mgcpStatisticsAvgConnection Time	Average connection time (in seconds) since the last restart. **Default Value**: 0
mgcpStatisticsTotalNumberOf Errors	The total number of errors since the last start up. **Default Value**: 0

Country Specific Parameters

The following parameters differ depending on the country you are in. Note that the *On – Off* sequence should be read as follows:

- **1.0** – 0.85 means that the sequence is 1.0 second On and 0.85 second Off.

Australia

The following parameters apply if you have selected Australia as location.

Table 57: Australia Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-20 dBm
Busy Tone	400 Hz	**0.375** – 0.375	-13 dBm
Ringing Tone	450 Hz + 450 Hz	**0.4** – 0.2 – **0.4** – 2.0	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-20 dBm
Ring	65 VRMS, 50 Hz	**0.4** – 2.0	
Impedance	Z_R = 220 Ω + 820 Ω // 120 nF		
Tbrl-Impedance	Z_N =220 Ω + 820 Ω // 120 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-6 dBr

Austria

The following parameters apply if you have selected Austria as location.

Table 58: Austria Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	450 Hz	**1.0** – 0.85	-20 dBm
Busy Tone	450 Hz	**0.45** – 0.45	-13 dBm
Ringing Tone	450 Hz	**1.0** – 4.0	-20 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-20 dBm
Ring	65 VRMS, 50 Hz	**1** – 5	
Impedance	Z_R = 270 Ω + 750 Ω // 150 nF		
Tbrl-Impedance	Z_N = 600 Ω		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-10 dBr

France

The following parameters apply if you have selected France as location.

Table 59: France Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	330 Hz	**CONTINUOUS**	-16.9 dBm
Busy Tone	440 Hz	**0.5** – 0.5	-19.9 dBm
Ringing Tone	440 Hz	**1.5** – 3.5	-19.9 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-19.9 dBm
Ring	75 VRMS, 50 Hz	**1.5** – 3.5	
Impedance	Z_R = 215 Ω + 1000 Ω // 137 nF		
Tbrl-Impedance	Z_N = 600 Ω		
FXS Line Attenuation (Input)			-1.9 dBr
FXS Line Attenuation (Output)			-8.9 dBr

Germany

The following parameters apply if you have selected Germany as location.

Table 60: Germany 1 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**0.2** – 0.3, **0.2** – 0.3, **0.2** – 0.8	-16 dBm
Busy Tone	425 Hz	**0.17** – 0.43	-16 dBm
Ringing Tone	425 Hz	**1.0** – 4.0, **1.0** – 4.0, **1.0** – 4.0	-16 dBm
Special Information Tone	425 Hz	**0.17**– 0.43	-16 dBm
Ring	75 VRMS, 25 Hz	**1** – 4	
Impedance	Z_R = 220 Ω + 820 Ω // 115 nF		
Tbrl-Impedance	Z_N = 220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-10 dBr

Table 61: Germany 2 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**0.2** – 0.3, **0.2** – 0.3, **0.2** – 0.8	-13 dBm
Busy Tone	425 Hz	**0.17** – 0.43	-13 dBm

Table 61: Germany 2 Parameters (Continued)

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Ringing Tone	425 Hz	**1.0** – 4.0, **1.0** – 4.0, **1.0** – 4.0	-13 dBm
Ring	75 VRMS, 25 Hz	**1** – 4	
Impedance	Z_R = 220 Ω + 820 Ω // 115 nF		
Tbrl-Impedance	Z_N = 220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Great Britain

The following parameters apply if you have selected Great Britain as location.

Table 62: Great Britain Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350+440 Hz	**CONTINUOUS**	-19 dBm
Busy Tone	400 Hz	**0.375** – 0.375	-19 dBm
Ringing Tone	400+450 Hz	**0.4** – 0.2, **0.4** – 2.0, **0.35** – 0.22 followed by **0.4** – 0.2, **0.4** – 2.0	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-19 dBm
Ring	62 VRMS, 25 Hz	**1.0** – 4.0	
Impedance	Z_R = 300 Ω + 1000 Ω // 220 nF		
Tbrl-impedance	Z_N = 370 Ω + 620 Ω // 310 nF		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-9 dBr

Italy

The following parameters apply if you have selected Italy as location.

Table 63: Italy Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425+350 Hz	**CONTINUOUS**	-13 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-13 dBm
Ringing Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-20 dBm
Ring	75 VRMS, 25 Hz	**1.0** – 4.0	
Impedance	Z_R = 180 Ω + 630 Ω // 60 nF		
Tbrl-impedance	Z_N = 750 Ω // 18 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Japan

The following parameters apply if you have selected Japan as location.

Table 64: Italy Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 Hz	**CONTINUOUS**	-20 dBm
Busy Tone	400 Hz	**0.5** – 0.5	-20 dBm
Ringing Tone	400 Hz	**1.0** – 2.0	-20 dBm
Special Information Tone	400 Hz	**0.1** – 1.0	-20 dBm
Recall Dial Tone	350 + 440 Hz	**CONTINUOUS**	-20 dBm
Ring	67 VRMS, 20 Hz	**1.0** – 2.0	
Impedance	Z_R = 600 Ω		
Tbrl-impedance	Z_N = 600 Ω		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

North America

The following parameters apply if you have selected North America as location.

Table 65: North America 1 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels (Level / Frequency)
Dial Tone	350+440 Hz	**CONTINUOUS**	-17 dBm
Busy Tone	440+620 Hz	**0.5** – 0.5	-21 dBm
Ringing Tone	440+480 Hz	**2.0** – 4.0	-16 dBm
Intercept Tone	440 Hz 620 Hz	**0.25** – 0.25 **0.25** – 0.25	-14 dBm
Ring	70 VRMS, 20 Hz	**2.0** – 4.0	
Impedance	Z_R = 600 Ω		
Tbrl-Impedance	Z_N = 600 Ω		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-3 dBr

Table 66: North America 2 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels (Level / Frequency)
Dial Tone	350+440 Hz	**CONTINUOUS**	-17 dBm
Busy Tone	440+620 Hz	**0.5** – 0.5	-21 dBm
Ringing Tone	440+480 Hz	**2.0** – 4.0	-16 dBm
Intercept Tone	440 Hz 620 Hz	**0.25** – 0.25 **0.25** – 0.25	-14 dBm
Ring	70 VRMS, 20 Hz	**2.0** – 4.0	
Impedance	Z_R = 600 Ω		
Tbrl-Impedance	Z_N = 350 Ω + 1000 Ω // 210 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			0 dBr

Spain

The following parameters apply if you have selected Spain as location.

Table 67: Spain Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**0.2** – 0.3, **0.2** – 0.3, **0.2** – 0.8	-10 dBm
Busy Tone	425 Hz	**0.2** – 0.2	-13 dBm
Ringing Tone	425 Hz	**1.5** – 3.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-20 dBm
Ring	75 VRMS, 25 Hz	**1.5** – 3.0	
Impedance	Z_R = 220 Ω + 820 Ω // 120 nF		
Tbrl-Impedance	Z_N = 220 Ω + 820 Ω // 120 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Switzerland

The following parameters apply if you have selected Switzerland as location.

Table 68: Switzerland Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-8 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-13 dBm
Ringing Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-13 dBm
Ring	70 VRMS, 25 Hz	**1.0** – 4.0	
Impedance	Z_R = 220 Ω + 820 Ω // 115 nF		
Tbrl-impedance	Z_N = 220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-6.5 dBr

Safety & EMI Certifications

This Appendix lists the various Safety and EMI certifications of the AT-VP504E FXS.

Safety & EMI Certifications Supported

The AT-VP504E FXS has received the following Safety & EMI Certifications:

- United States: FCC Part 15 class A; FCC Part 68 subpart D
- Canada: CS-03 Issue 8
- CE Mark: conformity with EMC Directive
- UL and UL-C
- CSA and CSA-US

Note: The Safety and EMI Certifications of the AT-VP504E FXS are printed on a sticker located on the bottom of the unit.

Disclaimers

Federal Communications Commission (FCC) Part 15

This equipment has been tested and found to comply with the limits for Class A Digital Device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Note: Any changes or modifications not expressly approved by Allied Telesyn could void the user's authority to operate the equipment.

Federal Communications Commission (FCC) Part 68

This equipment complies with Part 68 of the FCC Rules. On the underside of this equipment is a label that contains, among other information, the FCC Registration Number, Ringer Equivalence Number (REN) and USOC jack type for this equipment. You must, upon request, provide this information to your telephone company.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN's of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your telephone company to determine the maximum REN for your calling area. If your telephone equipment causes harm to the telephone network, the Telephone Company may discontinue your service temporarily. If possible, they will notify you in advance, but if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.

Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact Allied Telesyn for information on obtain service or repairs. The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company.

Connection to party lines is subject to state tariffs.

INSTALLATION

This device is equipped with an USOC RJ-11C connector.

Industry Canada

The Industry Canada Label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Warning: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Note: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Number of all the devices does not exceed 5.

10 BaseT An Ethernet local area network which works on twisted pair wiring.

100 BaseT A newer version of Ethernet that operates at 10 times the speed of a 10 BaseT Ethernet.

A-Law The ITU-T companding standard used in the conversion between analog and digital signals in PCM (Pulse Code Modulation) systems. A-law is used primarily in European telephone networks and contrasts with the North American mu (μ)-law standard. See also *mu (μ)-law*.

Area Code The preliminary digits that a user must dial to be connected to a particular outgoing trunk group or line. In North America, an Area Code has three (3) digits and is used with a NXX (office code) number. For example, in the North American telephone number *561-955-1212*, the numbers are defined as follows:

Table 69: North American Numbering Plan

No.	Description
561	Area Code, corresponding to a geographical zone in a non-LNP (Local Number Portability) network.
955	NXX (office code), which corresponds to a specific area such as a city region.
1212	Unique number to reach a specific destination.

Outside North America, the Area Code may have any number of digits, depending on the national telecommunication regulation of the country. In France, for instance, the numbering terminology is defined as *xZABPQ 12 34*, where:

Table 70: France Numbering Plan

No.	Description
x	Operator forwarding the call. This prefix can be made of 4 digits.
Z	(regional) geographical zone of the number (in France, there are 5 zones). It has two (2) digits.
ABPQ	First 4 digits corresponding to a local zone defined by central offices.

Table 70: France Numbering Plan (Continued)

No.	Description
12 34	Unique number to reach a specific destination.

In this context, the Area Code corresponds to the *Z* portion of the numbering plan. Since virtually every country has a different dialing plan nomenclature, it is recommended to identify the equivalent of an Area Code for the location of your communication unit.

Battery feed, Over-voltage protection, Ringing, Signalling, Coding, Hybrid, and Testing (BORSCHT) A group of functions provided to an analog line from a line circuit of a digital central office switch.

Call Agent (Connection Manager) Manages the connection state of the AT-VP504E FXS. The Connection Manager provides Basic Call Processing and MGCP Gateway Support.

Country Code (CC) In international direct telephone dialing, a code that consists of 1-, 2-, or 3-digit numbers in which the first digit designates the region and succeeding digits, if any, designate the country.

Custom Local Area Signalling Services (CLASS) One of an identified group of network-provided enhanced services. A CLASS group for a given network usually includes several enhanced service offerings, such as incoming-call identification, call trace, call blocking, automatic return of the most recent incoming call, call redial, and selective forwarding and programming to permit distinctive ringing for incoming calls.

Digital Signal Processor (DSP) Specialized computer chip designed to perform speedy and complex operations on digitized waveforms. Useful in processing sound (like voice phone calls) and video.

Domain Name Server (DNS) Internet service that translates domain names into IP addresses. To use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to 198.105.232.4.

Dual-Tone Multi-Frequency (DTMF) In telephone systems, multi-frequency signalling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher

	frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol “#” or “*”, the “*” being reserved for special purposes.
Dynamic Host Configuration Protocol (DHCP)	TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.
Echo Cancellation	Technique that allows for the isolation and filtering of unwanted signals caused by echoes from the main transmitted signal.
Electronically Erasable Programmable Read Only Memory (EEPROM)	A read only memory device which can be erased and reprogrammed. Typically, it is reprogrammed electronically (not electromagnetically) with ultraviolet light.
Erasable Programmable Read Only Memory (EPROM)	EPROM is a special type of memory that retains its contents until it is exposed to ultraviolet light. The ultraviolet light clears its contents, making it possible to reprogram the memory. To write to and erase an EPROM, you need a special device called a PROM programmer or PROM burner.
Far End Disconnect	This term refers to methods for detecting that a remote party has hung up. This is also known as Hangup Supervision. There are several methods that may be used by a PBX/ACD/CO to signal that the remote party has hung up, including cleardown tone, or a wink.
Federal Communications Commission (FCC)	U.S. government regulatory body for radio, television, and interstate telecommunications services and international services originating in the United States.
Foreign Exchange Service/Station (FXS)	A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., “foreign”, exchange, rather than the local exchange area’s central office. A FXS line is normally connected to a standard telephone, fax or modem.

G.711 ITU-T recommendation for an algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48, 56, and 64 Kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

G.723.1 A Codec that provides the greatest compression, 5.3 Kbps or 6.3 Kbps; typically specified for multimedia applications such as H.323 videoconferencing.

G.729/G.729A A Codec that provides near toll quality at a low delay which uses compression to 8 Kbps (8:1 compression rate).

Gateway A device that links two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

Integrated Services Digital Network (ISDN) An international telecommunications network, based on a set of communications standards, for digital transmission of voice, video, and data over WANs. ISDN interfaces also provide LAN connections and remote access capability. ISDN has two types of service: BRI (basic rate interface) and PRI (primary rate interface).

International Telecommunication Union (ITU) Organization based in Geneva, Switzerland, that is the most important telecom standards-setting body in the world.

Internet Protocol (IP) A standard describing software that keeps track of the Internet's addresses for different nodes, routes outgoing messages, and recognises incoming messages.

Jitter

1. A distortion caused by the variation of a signal from its references which can cause data transmission errors, particularly at high speeds.
2. Variations in amplitude, time, frequency or phase.

Layer 2 Layer 2 refers to the Data Link Layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The Data Link Layer is concerned with moving data across the physical links in the network.

The Data-Link Layer contains two sublayers that are described in the IEEE-802 LAN standards:

- Media Access Control (MAC)

- Logical Link Control (LLC)

Layer 3 Layer 3 refers to the Network layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The Network Layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding to the transport layer incoming messages for local host domains.

A router is a layer 3 device, although some newer switches also perform layer 3 functions. The Internet Protocol (Internet Protocol) address is a layer 3 address.

Light Emitting Diode (LED) A semiconductor diode that emits light when a current is passed through it.

Local Area Network (LAN) Data-only communications network confined to a limited geographic area, with moderate to high data rates. See also WAN.

Management Information Base (MIB) MIBs are specifications containing definitions of management information so that networked systems can be remotely monitored, configured and controlled.

Management Server It includes a web-based provisioning client, a provisioning server, and SNMP proxy server used to manage all agents connected to the system. The Management Server provides Gateway provisioning, Monitoring, and Numbering Plan.

Media Access Control (MAC) Address A layer 2 address, 6 bytes long, associated with a particular network device; used to identify devices in a network; also called hardware or physical address.

Media Gateway Control Protocol (MGCP) An application programming interface and a protocol for controlling Voice over IP (VoIP) Gateways from external call control elements, where the intelligence is.

Mu (μ)-Law The PCM (Pulse Code Modulation) voice coding and companding standard used in Japan and North America. See also *A-Law*.

Network A group of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances. A network can consist of any combination of local area networks (LAN) or wide area networks (WAN).

Off-hook A line condition caused when a telephone handset is removed from its cradle.

On-hook A line condition caused when a telephone handset is resting in its cradle.

Packet Includes three principal elements: control information (such as destination, origin, length of packet), data to be transmitted, and error detection and A group of bits, including data and control signals, arranged in a specific format and transmitted as a whole. The structure of a packet depends on the protocol.

Plain Old Telephone System (POTS) Standard telephone service used by most residential locations; basic service supplying standard single line telephones, telephone lines, and access to the public switched network.

Port Network access point, the identifier used to distinguish among multiple simultaneous connections to a host.

Portable Operating System Interface (POSIX) POSIX is a set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to be able to develop programs that could be moved among different manufacturer's computer systems without having to be recoded. UNIX was selected as the basis for a standard system interface partly because it was "manufacturer-neutral." However, several major versions of UNIX existed so there was a need to develop a common denominator system.

Private Branch Exchange (PBX) A small to medium sized telephone system and switch that provides communications between onsite telephones and exterior communications networks.

Programmable Read-Only Memory (PROM) A memory chip where data is written only once as it remains there forever. Unlike RAM, PROMs retain their contents when the computer is turned off.

Protocol A formal set of rules developed by international standards bodies, LAN equipment vendors, or groups governing the format, control, and timing of network communications. A set of conventions dealing with transmissions between two systems. Typically defines how to implement a group of services in one or two layers of the OSI reference model. Protocols can describe low-level details of machine-to-machine interfaces or high-level exchanges between allocation programs.

Proxy Server	An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.
Public Switched Telephone Network (PSTN)	The local telephone company network that carries voice data over analog telephone lines.
Quality of Service (QoS)	Quality of Service is a measure of the telephone service quality provided to a subscriber. This could be, for example, the longest time someone should wait after picking up the handset before they receive dial tone (three seconds in most U.S. states).
Realtime Transport Protocol (RTP)	An IETF standard for streaming realtime multimedia over IP in packets. Supports transport of real-time data like interactive voice and video over packet switched networks.
Registrar Server	A server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and MAY offer location services.
Router	A specialized switching device which allows customers to link different geographically dispersed local area networks and computer systems. This is achieved even though it encompasses different types of traffic under different protocols, creating a single, more efficient, enterprise-wide network.
Switched Circuit Network (SCN)	A communication network, such as the public switched telephone network (PSTN), in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices.
Server	A computer or device on a network that works in conjunction with a client to perform some operation, for example a Windows NT Server.
Session Initiation Protocol (SIP)	SIP is a simple signalling protocol for Internet conferencing and telephony.
Simple Network Management Protocol (SNMP)	A standard of network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol / Internet Protocol (TCP/IP) suite and defined in RFC 1157.

Simple Network Time Protocol (SNTP) SNTP, which is an adaptation of the Network Time Protocol (NTP), is widely used to synchronize computer clocks in the global Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time- synchronization subnet and adjust the local clock in each participating subnet peer. In most places of the Internet of today, NTP provides accuracies of 1-50 ms, depending on the characteristics of the synchronization source and network paths.

Stack A set of network protocol layers that work together. The OSI Reference Model that defines seven protocol layers is often called a stack, as is the set of TCP/IP protocols that define communication over the internet.

The term stack also refers to the actual software that processes the protocols. So, for example, programmers sometimes talk about loading a stack, which means to load the software required to use a specific set of protocols.

Subnet An efficient means of splitting packets into two fields to separate packets for local destinations from packets for remote destinations in TCP/IP networks.

T.38 An ITU-T Recommendation for Real-time fax over IP. T.38 addresses IP fax transmissions for IP-enabled fax devices and fax gateways, defining the translation of T.30 fax signals and Internet Fax Protocols (IFP) packets.

Telephony The science of translating sound into electrical signals, transmitting them, and then converting them back into sound.

Terminal Device capable of sending or receiving data over a data communications channel.

Transmission Control Protocol/Internet Protocol (TCP/IP) A suite of communications protocols developed by the Department of Defense in the 1970s that connects hosts on the Internet and provides the standards for transmitting data over networks.

Trivial File Transfer Protocol (TFTP) A simplified version of FTP that transfers files but does not provide password protection, provide directory capability, or allow transmission of multiple files with one command.

User Datagram Protocol (UDP) An efficient but unreliable, connectionless protocol that is layered over IP, as is TCP. Application programs are needed to supplement the protocol to provide error processing and retransmission of data. UDP is an OSI layer 4 protocol.

Voice Over IP (VoIP) The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

Wide Area Network (WAN) A large (geographically dispersed) network, usually constructed with serial lines, that covers a large geographic area. A WAN connects LANs using transmission lines provided by a common carrier.

Index

Numerics

10 BaseT 5, 17, 35, 129
100 BaseT 17, 35, 129
802.1q, in QoS 65

A

acronyms ix
A-Law 59, 129
analog modem, feature 3
area code 32, 129
authentication information 89

B

before you begin ix
BORSCHT 130
Bypass, System Failure 18, 53

C

call
    forward
        on busy 104
        on no answer 105
        unconditional 103
    placing 33
    transfer
        supervised 106
        unsupervised 106
    waiting 106
call agent
    definition 130
    requirement 11
    setting 110
caller ID 106
codec, setting preferred 59
configuration file 28
configuring the software
    changing parameters 30
    configuration file 28
    IP addresses 27
    MIB. see *SNMP*
    subnet mask 27
    using DHCP (dynamic) 35
    using Static 37
connecting the unit 17
connectors
    Bypass 5
    Default Settings 6
    Ethernet 5
    Phones/Faxes 5
    power 5
conventions, of the manual xi
country code 32
country specific parameters 119
    overriding 32
    setting 30

D

Default Settings
    factory settings procedure 24
    in recovery mode 22
DHCP server
    configuring 38
    definition 131
    entering IP addresses 41
    network configuration 39
    requirment 11
    vendor specific information 39
dial map
    # and * characters 93
    combining two expressions 93
    definition 91
    examples
        PBX emulation 99
        standard calls 96
    rules 94
    special characters 92
    timer 93
    using 92
    validating 94
Differentiated Services (DS) Field, in QoS 63
downloading software 43

E

echo cancel 57
emergency software download 49
Ethernet connection, setting speed 35

F

factory settings, reverting to 24
fax
    disabling the call waiting tone 106
    feature 3
features
    analog modem 3
    fax interface 3

FXS port 2
system failure bypass 3

G

G.711 59, 132
G.723.1 59, 132
G.729AB 59, 132
gateway 132

H

hardware
cleaning 79
condensation 79
front indicators 4
proper location 79
rear connections 5

I

IEEE 802.1q, in QoS 65
indicators of the hardware 4
installation
connecting the hardware 17
verifying 25
Internet Protocol (IP) 132
IP address
default settings 23
entering 41
MGCP call agent 110
SIP logging client 85
SIP servers 86
SNTP server 73
syslog daemon 68
TFTP server 45
Unit Manager 62
using DHCP 35
using static 37

J

jitter 132
jitter buffer protection 55

L

LAN 133
cable 25
Layer 2 132
Layer 3 133
LEDs
behavior in download mode 20, 48
definition 133
interpreting 19
interpreting in reset mode 20
LAN 19
Power 19
Test 19
location, setting country 30

M

management server 133
manual conventions xi
MGCP, setting
call agents 110
using DHCP information 110
using Static information 111
configuration 109
endpoints 112
packages
DTMF 115
Generic Media 114
Line 115
retransmission 112
services 110
statistics 117
status parameters 116
switching to 109
MIB
definition 7, 133
in SNMP protocol 6
see *parameters*
structure
MGCP MIB 8
Provisioning MIB 8
SIP MIB 8
mounting
on a rack 13
on a wall 14
stacking 17
unit 13
Mu (µ)-Law 59, 133

O

overview of the product 1

P

package contents 12
parameters
modifying 8, 30
placing a call 33
ports
country-specific variables 58
definition 134

DSP variables 55
echo cancel 57
jitter buffer protection 55
voice activity detection 56
enabling 55
preferred codec 59
user gain variables 57
product
overview 1
protocol, switching 9
provisioning
configuration file 28
initial sequence 21
MIB files 29
restart handler 29
troubleshooting 22

Q

QoS
Differentiated Services (DS) Field 63
IEEE 802.1q 65
VLAN 66

R

rack-mounting the unit 13
rear connections 5
recovery mode, resetting in 22
related documentation x
requirements 11

S

Safety & EMI Certifications
FCC Part 15 125
FCC Part 68 125
Industry Canada 126
signaling protocol
MGCP. see *MGCP, setting*
SIP. see *SIP, setting*
SIP, setting
configuration 85
Logging Client
enabling 85
using DHCP information 85
using Static information 86
SIP servers
using DHCP information 86
using Static information 87
SIP User Agents
authentification information 89
friendly name 88
main alias 88
other aliases 88
session timers 88
setting information 88
site, selecting for unit 12
SNMP 135
configuring 69
definition 6
MIB 6
types of messages 7
SNTP
enabling 72
time zone
defining custom 76
selecting 74
using DHCP information 73
using static information 73
software
downloading
configuring TFTP server 43
DHCP vs. Static Configuration 45
emergency procedure 49
LED states 48
procedure 46
software configuration 27, 30
stacking units 17
subnet mask
default IP address 23
subnet mask, configuring 27
switching protocol 9
Syslog daemon
configuring 69
definition 67
enabling 67
requirement 11
using DHCP information 68
using static information 68
System Failure Bypass
activate when connection to the server is lost 53
activate when Ethernet connection is lost 53
always activate 53
definition 53
System, Failure Bypass 3

T

telephony services
call forward
on busy 104
on no answer 105
unconditional 103
call transfer - supervised 106
call transfer - unsupervised 106
call waiting 106
caller ID 106

conference call 106
TFTP server
configuring 43
definition 136
requirement 11
using DHCP information 45
using Static information 46
time zone
defining custom 76
selecting 74
troubleshooting
all LED's are off 80
cannot make a call 80
cannot make a call to a destination 80
SNMP Network Management software can no longer access the unit 82
SNMP network management software cannot access the unit 81
solving general operations problems 80
solving software problems 81
traps are not received by the SNMP network manager 82

U

Unit Manager
using 61
using DHCP information 62
using Static information 62
using the unit 27

V

vendor specific information
codes 41
creating 39
verifying the installation 25
VLAN, in QoS 66
voice activity detection 56

W

wall-mounting the unit 14
what's new in this version ix